

Concessione per la 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

CIG: 9066973ECE

CUP: J51B21005710007

PROGETTO ESECUTIVO DI DETTAGLIO

SISTEMA INFORMATIVO SANITARIO INTEGRATO REGIONALE (SISaR)

Ares Sardegna - Azienda Regionale della Salute

CIG: B06937F577

SOMMARIO

1	PREMESSA	32
2	DOCUMENTI DI RIFERIMENTO	32
3	ACRONIMI	33
4	AMBIENTE TO-BE - PRODUZIONE	35
4.1	ASL 1 - SASSARI.....	35
4.1.1	Architettura	35
4.1.1.1	Schema Logico	37
4.1.1.2	Lista Componenti	37
4.1.2	Infrastruttura	38
4.1.2.1	Virtual Machine	39
4.1.2.1.1	Caratteristiche	39
4.1.2.1.2	Dimensionamento	39
4.1.2.1.3	Composizione Storage	40
4.1.2.1.4	Piano di Indirizzamento.....	40
4.1.2.1.5	Software Installato.....	41
4.1.2.1.6	Web Server	42
4.1.2.2	Database Server	43
4.1.2.3	DNS.....	43
4.1.2.4	Storage Condivisi.....	43
4.1.2.5	Networking.....	44
4.1.2.5.1	Schema di Rete	44
4.1.2.5.2	Bilanciamento	44
4.1.2.5.3	Reverse Proxy	45
4.1.2.5.4	Flussi e Accessibilità	46
4.1.2.6	Sicurezza.....	52

4.1.2.6.1	Autenticazione	52
4.1.2.6.2	Certificati SSL	54
4.1.2.6.3	Regole Firewall	54
4.1.2.7	Licenze	56
4.1.2.8	Policy di Backup	56
4.1.2.9	Policy di DR	59
4.2	ASL 2 – OLBIA	60
4.2.1	Architettura	60
4.2.1.1	Schema Logico	61
4.2.1.2	Lista Componenti	61
4.2.2	Infrastruttura	62
4.2.2.1	Virtual Machine	63
4.2.2.1.1	Caratteristiche	63
4.2.2.1.2	Dimensionamento	63
4.2.2.1.3	Composizione Storage	64
4.2.2.1.4	Piano di Indirizzamento.....	64
4.2.2.1.5	Software Installato.....	65
4.2.2.1.6	Web Server	66
4.2.2.2	Database Server	66
4.2.2.3	DNS.....	66
4.2.2.4	Storage Condivisi.....	67
4.2.2.5	Networking	67
4.2.2.5.1	Schema di Rete	67
4.2.2.5.2	Bilanciamento	67
4.2.2.5.3	Reverse Proxy	69
4.2.2.5.4	Flussi e Accessibilità	69

4.2.2.5.5	Accessi esterni/interni	76
4.2.2.6	Sicurezza	76
4.2.2.6.1	Autenticazione	76
4.2.2.6.2	Certificati SSL	76
4.2.2.6.3	Regole Firewall	77
4.2.2.7	Licenze	79
4.2.2.8	Policy di Backup	79
4.2.2.9	Policy di DR	82
4.3	ASL 3 – NUORO	83
4.3.1	Architettura	83
4.3.1.1	Schema Logico	84
4.3.1.2	Lista Componenti	84
4.3.2	Infrastruttura	85
4.3.2.1	Virtual Machine	86
4.3.2.1.1	Caratteristiche	86
4.3.2.1.2	Dimensionamento	86
4.3.2.1.3	Composizione Storage	87
4.3.2.1.4	Piano di Indirizzamento.....	87
4.3.2.1.5	Software Installato.....	88
4.3.2.1.6	Web Server	89
4.3.2.2	Database Server	90
4.3.2.3	DNS.....	90
4.3.2.4	Storage Condivisi.....	90
4.3.2.5	Networking	91
4.3.2.5.1	Schema di Rete	91
4.3.2.5.2	Bilanciamento.....	91

4.3.2.5.3	Reverse Proxy	92
4.3.2.5.4	Flussi e Accessibilità	93
4.3.2.5.5	Accessi esterni/interni	99
4.3.2.6	Sicurezza	100
4.3.2.6.1	Autenticazione	100
4.3.2.6.2	Certificati SSL	100
4.3.2.6.3	Regole Firewall	100
4.3.2.7	Licenze	102
4.3.2.8	Policy di Backup	102
4.3.2.9	Policy di DR	106
4.4	ASL 4 – LANUSEI	107
4.4.1	Architettura	107
4.4.1.1	Schema Logico	108
4.4.1.2	Lista Componenti	108
4.4.2	Infrastruttura	109
4.4.2.1	Virtual Machine	110
4.4.2.1.1	Caratteristiche	110
4.4.2.1.2	Dimensionamento	110
4.4.2.1.3	Composizione Storage	111
4.4.2.1.4	Piano di Indirizzamento	111
4.4.2.1.5	Software Installato	112
4.4.2.1.6	Web Server	113
4.4.2.2	Database Server	113
4.4.2.3	DNS	113
4.4.2.4	Storage Condivisi	114
4.4.2.5	Networking	114

4.4.2.5.1	Schema di Rete	114
4.4.2.5.2	Bilanciamento	114
4.4.2.5.3	Reverse Proxy	116
4.4.2.5.4	Accessi esterni/interni	116
4.4.2.5.5	Flussi e Accessibilità	123
4.4.2.6	Sicurezza	123
4.4.2.6.1	Autenticazione	123
4.4.2.6.2	Certificati SSL	123
4.4.2.6.3	Regole Firewall	124
4.4.2.7	Licenze	126
4.4.2.8	Policy di Backup	126
4.4.2.9	Policy di DR	129
4.5	ASL 5 – ORISTANO	130
4.5.1	Architettura	130
4.5.1.1	Schema Logico	131
4.5.1.2	Lista Componenti	131
4.5.2	Infrastruttura	132
4.5.2.1	Virtual Machine	133
4.5.2.1.1	Caratteristiche	133
4.5.2.1.2	Dimensionamento	133
4.5.2.1.3	Composizione Storage	134
4.5.2.1.4	Piano di Indirizzamento.....	134
4.5.2.1.5	Software Installato.....	135
4.5.2.1.6	Web Server	136
4.5.2.2	Database Server	136
4.5.2.3	DNS.....	136

4.5.2.4	Storage Condivisi.....	137
4.5.2.5	Networking.....	137
4.5.2.5.1	Schema di Rete	137
4.5.2.5.2	Bilanciamento.....	137
4.5.2.5.3	Reverse Proxy	139
4.5.2.5.4	Flussi e Accessibilità	139
4.5.2.5.5	Accessi esterni/interni	145
4.5.2.6	Sicurezza.....	146
4.5.2.6.1	Autenticazione.....	146
4.5.2.6.2	Certificati SSL.....	146
4.5.2.6.3	Regole Firewall	146
4.5.2.7	Licenze.....	149
4.5.2.8	Policy di Backup	149
4.5.2.9	Policy di DR.....	152
4.6	ASL 6 – SANLURI	153
4.6.1	Architettura	153
4.6.1.1	Schema Logico	154
4.6.1.2	Lista Componenti	154
4.6.2	Infrastruttura.....	154
4.6.2.1	Virtual Machine	155
4.6.2.1.1	Caratteristiche	155
4.6.2.1.2	Dimensionamento	156
4.6.2.1.3	Composizione Storage	156
4.6.2.1.4	Piano di Indirizzamento.....	157
4.6.2.1.5	Software Installato.....	158
4.6.2.1.6	Web Server	159

4.6.2.2	Database Server	159
4.6.2.3	DNS.....	159
4.6.2.4	Storage Condivisi.....	160
4.6.2.5	Networking	160
4.6.2.5.1	Schema di Rete	160
4.6.2.5.2	Bilanciamento	160
4.6.2.5.3	Reverse Proxy	161
4.6.2.5.4	Flussi e Accessibilità	162
4.6.2.5.5	Accessi esterni/interni	168
4.6.2.6	Sicurezza	168
4.6.2.6.1	Autenticazione	168
4.6.2.6.2	Certificati SSL	168
4.6.2.6.3	Regole Firewall	169
4.6.2.7	Licenze.....	171
4.6.2.8	Policy di Backup	171
4.6.2.9	Policy di DR	174
4.7	ASL 7 – CARBONIA	175
4.7.1	Architettura	175
4.7.1.1	Schema Logico	176
4.7.1.2	Lista Componenti	176
4.7.2	Infrastruttura	177
4.7.2.1	Virtual Machine	178
4.7.2.1.1	Caratteristiche	178
4.7.2.1.2	Dimensionamento	178
4.7.2.1.3	Composizione Storage	179
4.7.2.1.4	Piano di Indirizzamento.....	179

4.7.2.1.5	Software Installato.....	180
4.7.2.1.6	Web Server	181
4.7.2.2	Database Server	181
4.7.2.3	DNS.....	181
4.7.2.4	Storage Condivisi.....	182
4.7.2.5	Networking.....	182
4.7.2.5.1	Schema di Rete	182
4.7.2.5.2	Bilanciamento	182
4.7.2.5.3	Reverse Proxy	183
4.7.2.5.4	Flussi e Accessibilità	184
4.7.2.5.5	Accessi esterni/interni	190
4.7.2.6	Sicurezza.....	190
4.7.2.6.1	Autenticazione.....	190
4.7.2.6.2	Certificati SSL.....	190
4.7.2.6.3	Regole Firewall	191
4.7.2.7	Licenze.....	193
4.7.2.8	Policy di Backup	193
4.7.2.9	Policy di DR.....	196
4.8	ASL 8 – CAGLIARI	197
4.8.1	Architettura	197
4.8.1.1	Schema Logico	198
4.8.1.2	Lista Componenti	198
4.8.2	Infrastruttura.....	199
4.8.2.1	Virtual Machine	200
4.8.2.1.1	Caratteristiche	200
4.8.2.1.2	Dimensionamento	200

4.8.2.1.3	Composizione Storage	201
4.8.2.1.4	Piano di Indirizzamento.....	201
4.8.2.1.5	Software Installato.....	202
4.8.2.1.6	Web Server	203
4.8.2.2	Database Server	204
4.8.2.3	DNS.....	204
4.8.2.4	Storage Condivisi.....	204
4.8.2.5	Networking	205
4.8.2.5.1	Schema di Rete	205
4.8.2.5.2	Bilanciamento.....	205
4.8.2.5.3	Reverse Proxy	206
4.8.2.5.4	Flussi e Accessibilità.....	207
4.8.2.5.5	Accessi esterni/interni	213
4.8.2.6	Sicurezza.....	213
4.8.2.6.1	Autenticazione.....	213
4.8.2.6.2	Certificati SSL	213
4.8.2.6.3	Regole Firewall	214
4.8.2.7	Licenze.....	216
4.8.2.8	Policy di Backup	216
4.8.2.9	Policy di DR	219
4.9	ARNAS.....	220
4.9.1	Architettura	220
4.9.1.1	Schema Logico	221
4.9.1.2	Lista Componenti	221
4.9.2	Infrastruttura	222
4.9.2.1	Virtual Machine	222

4.9.2.1.1	Caratteristiche	222
4.9.2.1.2	Dimensionamento	223
4.9.2.1.3	Composizione Storage	223
4.9.2.1.4	Piano di Indirizzamento.....	223
4.9.2.1.5	Software Installato.....	225
4.9.2.1.6	Web Server	227
4.9.2.2	Database Server	227
4.9.2.3	DNS.....	227
4.9.2.4	Storage Condivisi.....	228
4.9.2.5	Networking	228
4.9.2.5.1	Schema di Rete	228
4.9.2.5.2	Bilanciamento	228
4.9.2.5.3	Reverse Proxy	229
4.9.2.5.4	Flussi e Accessibilità	230
4.9.2.5.5	Accessi esterni/interni	237
4.9.2.5.6	Sicurezza.....	238
4.9.2.5.7	Autenticazione	238
4.9.2.5.8	Certificati SSL	238
4.9.2.5.9	Regole Firewall	238
4.9.2.6	Licenze	240
4.9.2.7	Policy di Backup	240
4.9.2.8	Policy di DR	244
4.10	AOU CAGLIARI	245
4.10.1	Architettura	245
4.10.1.1	Schema Logico	246
4.10.1.2	Lista Componenti	246

4.10.2	Infrastruttura	246
4.10.2.1	Virtual Machine.....	247
4.10.2.1.1	Caratteristiche.....	247
4.10.2.1.2	Dimensionamento.....	247
4.10.2.1.3	Composizione Storage	248
4.10.2.1.4	Piano di Indirizzamento	248
4.10.2.1.5	Software Installato	249
4.10.2.1.6	Web Server.....	251
4.10.2.2	Database Server	251
4.10.2.3	DNS.....	251
4.10.2.4	Storage Condivisi.....	251
4.10.2.5	Networking	252
4.10.2.5.1	Schema di Rete.....	252
4.10.2.5.2	Bilanciamento	252
4.10.2.5.3	Reverse Proxy.....	253
4.10.2.5.4	Flussi e Accessibilità.....	253
4.10.2.5.5	Accessi esterni/interni	260
4.10.2.6	Sicurezza	260
4.10.2.6.1	Autenticazione	260
4.10.2.6.2	Certificati SSL.....	260
4.10.2.6.3	Regole Firewall	260
4.10.2.7	Licenze	261
4.10.2.8	Policy di Backup	261
4.10.2.9	Policy di DR	264
4.11	AOU SASSARI.....	265
4.11.1	Architettura	265

4.11.1.1.1	Schema Logico.....	266
4.11.1.1.2	Lista Componenti.....	266
4.11.2	Infrastruttura	267
4.11.2.1	Virtual Machine.....	267
4.11.2.1.1	Caratteristiche.....	267
4.11.2.1.2	Dimensionamento	268
4.11.2.1.3	Composizione Storage	268
4.11.2.1.4	Piano di Indirizzamento	268
4.11.2.1.5	Software Installato	270
4.11.2.1.6	Web Server.....	271
4.11.2.2	Database Server	272
4.11.2.3	DNS.....	272
4.11.2.4	Storage Condivisi.....	272
4.11.2.5	Networking	272
4.11.2.5.1	Schema di Rete.....	273
4.11.2.5.2	Bilanciamento	273
4.11.2.5.3	Reverse Proxy.....	274
4.11.2.5.4	Flussi e Accessibilità.....	274
4.11.2.6	Sicurezza	282
4.11.2.6.1	Autenticazione	282
4.11.2.6.2	Certificati SSL.....	282
4.11.2.6.3	Regole Firewall	282
4.11.2.7	Licenze	282
4.11.2.8	Policy di Backup	282
4.11.2.9	Policy di DR	286
4.12	CRESSAN	287

4.12.1	Architettura	287
4.12.1.1	Schema Logico	288
4.12.1.2	Lista Componenti	288
4.12.2	Infrastruttura	288
4.12.2.1	Virtual Machine.....	289
4.12.2.1.1	Caratteristiche.....	289
4.12.2.1.2	Dimensionamento	290
4.12.2.1.3	Composizione Storage	291
4.12.2.1.4	Piano di Indirizzamento	291
4.12.2.1.5	Software Installato	293
4.12.2.1.6	Web Server.....	294
4.12.2.2	Database Server	295
4.12.2.3	DNS.....	295
4.12.2.4	Storage Condivisi.....	296
4.12.2.5	Networking	296
4.12.2.5.1	Schema di Rete.....	296
4.12.2.5.2	Bilanciamento	296
4.12.2.5.3	Reverse Proxy.....	299
4.12.2.5.4	Flussi e Accessibilità.....	299
4.12.2.6	Sicurezza	302
4.12.2.6.1	Autenticazione	302
4.12.2.6.2	Certificati SSL.....	302
4.12.2.6.3	Micro-segmentazione.....	303
4.12.2.6.4	Regole Firewall	305
4.12.2.7	Licenze	310
4.12.2.8	Policy di Backup	311

4.12.2.9	Policy di DR	314
5	STRATEGIA DI MIGRAZIONE	315
5.1	PIANIFICAZIONE DELLA MIGRAZIONE	317
5.2	PREDISPOSIZIONE AMBIENTI TO-BE	317
5.2.1	Configurazione Ambiente.....	317
5.2.2	Migrazione Workload.....	318
5.3	MIGRAZIONE DATI	320
5.3.1	Modalità di Migrazione – Golden Gate	320
5.3.2	Primo Mock	323
6	COLLAUDO.....	324
6.1	Test List Piattaforma Applicativa SISaR	324
7	CUTOVER - GOLDEN GATE E POWERED-ON.....	343
7.1	Pre-cutover	343
7.2	Cutover	345
8	ORGANIZZAZIONE.....	347
9	ANALISI RISCHI.....	348
10	MONITORAGGIO.....	348

INDICE DELLE TABELLE

Tabella 1 - Informazioni Documento	31
Tabella 2 - Autore	31
Tabella 3 - Revisore.....	31
Tabella 4 - Approvatore	31
Tabella 5 - Documenti Contrattuali	32
Tabella 6 - Acronimi.....	35
Tabella 7 – Lista componenti ASL1	37
Tabella 8 – Caratteristiche ASL1	39
Tabella 9 – Dimensionamento ASL1	39
Tabella 10 – Composizione storage ASL1.....	40
Tabella 11 – Piano di indirizzamento ASL1.....	40
Tabella 12 – Software installato ASL1.....	42
Tabella 13 – Web Server ASL1	42
Tabella 14 – Database Server ASL1.....	43
Tabella 15 - Server DNS ASL1	43
Tabella 16 – Storage condivisi ASL1.....	43
Tabella 17 – Bilanciamento ASL1.....	44
Tabella 18 – Tipo keepalive ASL1.....	45
Tabella 19 – Tipo persistenza sessione ASL1.....	45
Tabella 20 – Tipologia balancing ASL1	45
Tabella 21 – Tipo domain Enable ASL1	45
Tabella 22 – Type ASL1.....	45
Tabella 23 – Reverse proxy ASL1	45
Tabella 24 – Flussi SIOAAP ASL1	47
Tabella 25 – Flussi SIOAAP – Connessioni a DB ASL1.....	47

Tabella 26 – Flussi DNS ASL1	48
Tabella 27 – Flussi SIOAAP ASL1	49
Tabella 28 – Flussi SIOAAP – Connessioni a DB ASL1.....	49
Tabella 29 – Flussi PICASSO ASL1	51
Tabella 30 – Flussi PICASSO – Connessioni a DB ASL1	51
Tabella 31 – Flussi SPAGIC ASL1	52
Tabella 32 – Accessi esterni/interni ASL1	52
Tabella 33 – Regole Firewall ASL1	56
Tabella 34 – Policy di backup ASL1	59
Tabella 35 – Lista componenti ASL2	61
Tabella 36 – Caratteristiche ASL2	63
Tabella 37 – Dimensionamento ASL2	63
Tabella 38 – Composizione storage ASL2.....	64
Tabella 39 – Piano di indirizzamento ASL2.....	64
Tabella 40 – Software installato	65
Tabella 41 – Web server ASL2	66
Tabella 42 – Database Server ASL2.....	66
Tabella 43 - Server DNS ASL2	66
Tabella 44 – Storage condivisi ASL2.....	67
Tabella 45 – Bilanciamento ASL2.....	68
Tabella 46 – Tipo keepalive ASL2.....	68
Tabella 47 – Tipo persistenza sessione ASL2.....	68
Tabella 48 – Tipologia balancing ASL2	68
Tabella 49 – Tipo domain Enable ASL2	68
Tabella 50 – Type ASL2.....	68
Tabella 51 – Reverse proxy ASL2	69

Tabella 52 – Flussi SIOAPP ASL2	71
Tabella 53 – Flussi SIOAAP – Connessioni a DB ASL2.....	71
Tabella 54 – Flussi DNS ASL2	72
Tabella 55 – Flussi SIOAPP ASL2	73
Tabella 56 – Flussi SIOAAP – Connessioni a DB ASL2.....	73
Tabella 57 – Flussi Picasso.....	74
Tabella 58 – Flussi PICASSO – Connessioni a DB ASL2	75
Tabella 59 – Flussi SPAGIC ASL2	75
Tabella 60 – Accessi esterni/interni ASL2	76
Tabella 61 – Regole Firewall ASL2	78
Tabella 62 – Policy di backup ASL2	82
Tabella 63 – Lista componenti ASL3	84
Tabella 64 – Caratteristiche ASL3	86
Tabella 65 – Dimensionamento ASL3	87
Tabella 66 – Composizione storage ASL3.....	87
Tabella 67 – Piano di indirizzamento ASL3.....	88
Tabella 68 – Software installato ASL3.....	89
Tabella 69 – Web server ASL3	89
Tabella 70 – Database server ASL3	90
Tabella 71 - Server DNS ASL3	90
Tabella 72 – Storage condivisi ASL3.....	90
Tabella 73 – Bilanciamento ASL3.....	91
Tabella 74 – Tipo keepalive ASL3.....	91
Tabella 75 – Tipo persistenza sessione ASL3.....	92
Tabella 76 – Tipologia balancing ASL3	92
Tabella 77 – Tipo domain Enable ASL3	92

Tabella 78 – Type ASL3.....	92
Tabella 79 – Reverse Proxy ASL3	92
Tabella 80 – Flussi SIOAAP ASL3	94
Tabella 81 – Flussi SIOAAP – Connessioni a DB ASL3.....	94
Tabella 82 – Flussi DNS ASL3	95
Tabella 83 – Flussi SIOAAP ASL3	96
Tabella 84 – Flussi SIOAAP – Connessioni a DB ASL3.....	96
Tabella 85 – Flussi PICASSO ASL3	97
Tabella 86 – Flussi PICASSO – Connessioni a DB ASL3	99
Tabella 87 – Flussi SPAGIC ASL3	99
Tabella 88 – Accessi esterni/interni ASL3.....	100
Tabella 89 – Regole firewall ASL3	102
Tabella 90 – Policy di backup ASL3	106
Tabella 91 – Lista componenti ASL4	108
Tabella 92 – Caratteristiche ASL4	110
Tabella 93 – Dimensionamento ASL4	110
Tabella 94 – Composizione storage ASL4.....	111
Tabella 95 – Piano di indirizzamento ASL4.....	111
Tabella 96 – Software installato ASL4.....	112
Tabella 97 – Web server ASL4	113
Tabella 98 – Database server ASL4.....	113
Tabella 99 - Server DNS ASL4	113
Tabella 100 – Storage condivisi ASL4.....	114
Tabella 101 – Bilanciamento ASL4.....	115
Tabella 102 – Tipo keepalive ASL4.....	115
Tabella 103 – Tipo persistenza sessione ASL4.....	115

Tabella 104 – Tipologia balancing ASL4	115
Tabella 105 – Tipo domain Enable ASL4	115
Tabella 106 – Type ASL4.....	115
Tabella 107 – Reverse proxy ASL4	116
Tabella 108 – Accessi esterni/interni ASL4	116
Tabella 109 – Flussi SIOAAP ASL4	118
Tabella 110 – Flussi SIOAAP – Connessioni a DB	118
Tabella 111 – Flussi DNS ASL4	119
Tabella 112 – Flussi SIOAAP ASL4	119
Tabella 113 – Flussi SIOAAP – Connessioni a DB ASL4.....	120
Tabella 114 – Flussi PICASSO ASL4.....	121
Tabella 115 – Flussi PICASSO – Connessioni a DB ASL4	122
Tabella 116 – Flussi SPAGIC ASL4	123
Tabella 117 – Regole firewall ASL4	125
Tabella 118 – Policy di backup ASL4	129
Tabella 119 – Lista componenti ASL5	131
Tabella 120 – Caratteristiche ASL5	133
Tabella 121 – Dimensionamento ASL5	133
Tabella 122 – Composizione storage ASL5.....	134
Tabella 123 – Piano di indirizzamento ASL5.....	134
Tabella 124 – Software installato ASL5.....	135
Tabella 125 – Web server ASL5	136
Tabella 126 – Database server ASL5	136
Tabella 127 - Server DNS ASL5	136
Tabella 128 – Storage Condivisi ASL5	137
Tabella 129 – Bilanciamento ASL5.....	138

Tabella 130 – Tipo keepalive ASL5.....	138
Tabella 131 – Tipo persistenza sessione ASL5.....	138
Tabella 132 – Tipologia balancing ASL5	138
Tabella 133 – Tipo domain Enable ASL5	138
Tabella 134 – Type ASL5.....	138
Tabella 135 – Reverse proxy ASL5	139
Tabella 136 – Flussi SIOAAP ASL5	140
Tabella 137 – Flussi SIOAAP – Connessioni a DB ASL5.....	141
Tabella 138 – Flussi DNS ASL5	141
Tabella 139 – Flussi SIOAAP ASL5	142
Tabella 140 – Flussi SIOAAP – Connessioni a DB ASL5.....	142
Tabella 141 – Flussi PICASSO ASL5.....	144
Tabella 142 – Flussi PICASSO – Connessioni a DB ASL5	144
Tabella 143 – Flussi SPAGIC ASL5	145
Tabella 144 – Accessi esterni/interni ASL5	146
Tabella 145 – Regole firewall ASL5	148
Tabella 146 – Policy di backup ASL5	152
Tabella 147 – Lista componenti ASL6	154
Tabella 148 – Caratteristiche ASL6	156
Tabella 149 – Dimensionamento ASL6	156
Tabella 150 – Composizione storage ASL6.....	156
Tabella 151 – Piano di indirizzamento ASL6.....	157
Tabella 152 – Software installato ASL6.....	158
Tabella 153 – Web server ASL6	159
Tabella 154 – Database server ASL6	159
Tabella 155 - Server DNS ASL6	159

Tabella 156 – Storage condivisi ASL6.....	160
Tabella 157 – Bilanciamento ASL6.....	160
Tabella 158 – Tipo keepalive ASL6.....	161
Tabella 159 – Tipo persistenza sessione ASL6.....	161
Tabella 160 – Tipologia balancing ASL6.....	161
Tabella 161 – Tipo domain enable ASL6	161
Tabella 162 – Type- ASL6	161
Tabella 163 – Reverse proxy ASL6	161
Tabella 164 – Flussi SIOAAP ASL6	163
Tabella 165 – Flussi SIOAAP – Connessioni a DB ASL6.....	163
Tabella 166 – Flussi DNS ASL6	164
Tabella 167 – Flussi SIOAAP ASL6	165
Tabella 168 – Flussi SIOAAP – Connessioni a DB ASL6.....	165
Tabella 169 – Flussi PICASSO	166
Tabella 170 – Flussi PICASSO – Connessioni a DB ASL6	167
Tabella 171 – Accessi esterni/interni ASL6	168
Tabella 172 – Regole firewall ASL6	170
Tabella 173 – Policy di backup ASL6	174
Tabella 174 – Lista componenti ASL7	176
Tabella 175 – Caratteristiche ASL7	178
Tabella 176 – Dimensionamento ASL7	178
Tabella 177 – Composizione Storage ASL7.....	179
Tabella 178 – Piano di indirizzamento ASL7.....	179
Tabella 179 – Software installato ASL7	180
Tabella 180 – Web server ASL7	181
Tabella 181 – Database server ASL7	181

Tabella 182 - Server DNS ASL7	181
Tabella 183 – Storage Condivisi ASL7	182
Tabella 184 – Bilanciamento ASL7	182
Tabella 185 – Tipo keepalive ASL7	182
Tabella 186 – Tipo persistenza sessione ASL7	183
Tabella 187 – Tipologia balancing ASL7	183
Tabella 188 – Tipo domain enable ASL7	183
Tabella 189 – Type ASL7	183
Tabella 190 – Reverse proxy ASL7	183
Tabella 191 – Flussi SIOAAP ASL7	185
Tabella 192 – Flussi SIOAAP – Connessioni a DB ASL7	185
Tabella 193 – Flussi DNS ASL7	186
Tabella 194 – Flussi SIOAAP ASL7	187
Tabella 195 – Flussi SIOAAP – Connessioni a DB ASL7	187
Tabella 196 – Flussi PICASSO ASL7	188
Tabella 197 – Flussi PICASSO – Connessioni a DB ASL7	189
Tabella 198 – Accessi esterni/interni ASL7	190
Tabella 199 – Regole firewall ASL7	192
Tabella 200 – Policy di backup ASL7	196
Tabella 201 – Lista componenti ASL8	198
Tabella 202 – Caratteristiche ASL8	200
Tabella 203 – Dimensionamento ASL8	200
Tabella 204 – Composizione storage ASL8	201
Tabella 205 – Piano di indirizzamento ASL8	201
Tabella 206 – Software installato ASL8	203
Tabella 207 – Web Server ASL8	204

Tabella 208 – Database server ASL8	204
Tabella 209 - Server DNS ASL8	204
Tabella 210 – Storage condivisi ASL8.....	204
Tabella 211 – Bilanciamento ASL8.....	205
Tabella 212 – Tipo keepalive ASL8.....	205
Tabella 213 – Tipo persistenza sessione ASL8.....	206
Tabella 214 – Tipologia balancing ASL8	206
Tabella 215 – Tipo domain enable ASL8	206
Tabella 216 – Type ASL8.....	206
Tabella 217 – Reverse proxy ASL8	206
Tabella 218 – Flussi SIOAAP ASL8	208
Tabella 219 – Flussi SIOAAP – Connessioni a DB ASL8.....	208
Tabella 220 – Flussi DNS ASL8	209
Tabella 221 – Flussi SIOAAP	210
Tabella 222 – Flussi SIOAAP – Connessioni a DB ASL8.....	210
Tabella 223 – Flussi PICASSO ASL8.....	211
Tabella 224 – Flussi PICASSO Connessione a DB - ASL8	212
Tabella 225 – Flussi SPAGIC ASL8	212
Tabella 226 – Accessi esterni/interni ASL8	213
Tabella 227 – Regole firewall ASL8	215
Tabella 228 – Policy di backup ASL8	219
Tabella 229 – Lista Componenti ARNAS.....	221
Tabella 230 – Caratteristiche ARNAS.....	222
Tabella 231 – Dimensionamento ARNAS	223
Tabella 232 – Composizione Storage ARNAS	223
Tabella 233 – Piano di indirizzamento ARNAS.....	224

Tabella 234 – Software installato ARNAS.....	227
Tabella 235 – Web server ARNAS.....	227
Tabella 236 – Database server ARNAS.....	227
Tabella 237 - Server DNS ARNAS	228
Tabella 238 – Storage condivisi ARNAS.....	228
Tabella 239 – Bilanciamento ARNAS.....	229
Tabella 240 – Tipo keepalive ARNAS.....	229
Tabella 241 – Tipo persistenza sessione ARNAS.....	229
Tabella 242 – Tipologia balancing ARNAS	229
Tabella 243 – Domain enable ARNAS	229
Tabella 244 – Type ARNAS	229
Tabella 245 – Reverse proxy ARNAS.....	229
Tabella 246 – Flussi SIOAAP ARNAS.....	230
Tabella 247 – Flussi SIOAAP – Connessioni a DB ARNAS.....	231
Tabella 248 – Flussi DNS ARNAS.....	231
Tabella 249 – Flussi SIOAAP ARNAS.....	232
Tabella 250 – Flussi SIOAAP – Connessioni a DB ARNAS.....	233
Tabella 251 – Flussi PICASSO ARNAS	234
Tabella 252 - Flussi PICASSO – Connessioni a DB ARNAS.....	235
Tabella 253 – Flussi SPAGIC ARNAS	237
Tabella 254 – Accessi esterni/interni ARNAS	238
Tabella 255 – Regole firewall ARNAS.....	240
Tabella 256 – Policy di backup ARNAS.....	244
Tabella 257 – Lista componenti AOU CAGLIARI	246
Tabella 258 – Caratteristiche AOU CAGLIARI	247
Tabella 259 – Dimensionamento AOU CAGLIARI	247

Tabella 260 – Composizione storage AOU CAGLIARI	248
Tabella 261 – Piano di Indirizzamento AOU CAGLIARI.....	248
Tabella 262 – Software Installato AOU CAGLIARI.....	250
Tabella 263 – Web Server AOU CAGLIARI	251
Tabella 264 – Database server AOU CAGLIARI	251
Tabella 265 – DNS.....	251
Tabella 266 – Storage condivisi	252
Tabella 267 – Bilanciamento AOU CAGLIARI.....	252
Tabella 268 – Tipo keepalive AOU CAGLIARI.....	252
Tabella 269 – Tipo persistenza sessione AOU CAGLIARI.....	252
Tabella 270 – Tipologia balancing AOU CAGLIARI	252
Tabella 271 – Tipologia domain enable AOU CAGLIARI.....	253
Tabella 272 – Type AOU CAGLIARI.....	253
Tabella 273 – Reverse Proxy AOU CAGLIARI	253
Tabella 274 – Flussi SIOAAP AOU CAGLIARI	255
Tabella 275 – Flussi SIOAAP – Connessioni a DB AOU CAGLIARI.....	255
Tabella 276 – Flussi DNS AOU CAGLIARI	256
Tabella 277 – Flussi SIOAAP AOU CAGLIARI	257
Tabella 278 – Flussi SIOAAP – Connessioni a DB AOU CAGLIARI.....	258
Tabella 279 – Flussi PICASSO AOU CAGLIARI	259
Tabella 280 – Flussi PICASSO – Connessioni a DB AOU CAGLIARI	260
Tabella 281 – Accessi esterni/interni AOU CAGLIARI	260
Tabella 282 – Regole firewall AOU CAGLIARI	261
Tabella 283 – Policy di backup AOU CAGLIARI	264
Tabella 284 – Lista componenti AOU SASSARI	267
Tabella 285 – Caratteristiche AOU SASSARI.....	267

Tabella 286 – Dimensionamento AOU SASSARI	268
Tabella 287 – Composizione storage AOU Sassari.....	268
Tabella 288 – Piano di indirizzamento AOU SASSARI	269
Tabella 289 – Software installato AOU SASSARI.....	271
Tabella 290 – Web Server AOU SASSARI.....	271
Tabella 291 – Database server AOU SASSARI.....	272
Tabella 292 - Server DNS AOU SASSARI	272
Tabella 293 – Storage condivisi AOU SASSARI.....	272
Tabella 294 – Bilanciamento AOU SASSARI.....	273
Tabella 295 – Tipo keepalive AOU SASSARI	273
Tabella 296 – Tipo persistenza sessione AOU SASSARI.....	273
Tabella 297 – Tipologia balancing AOU SASSARI	273
Tabella 298 – Tipo domain enable AOU SASSARI	273
Tabella 299 – Type AOU SASSARI	274
Tabella 300 – Reverse proxyReverse proxy.....	274
Tabella 301 – Flussi SIOAAP AOU SASSARI.....	276
Tabella 302 – Flussi SIOAAP – Connessioni a DB AOU SASSARI	277
Tabella 303 – Flussi DNS AOU SASSARI.....	277
Tabella 304 – Flussi SIOAAP AOU SASSARI.....	278
Tabella 305 – Flussi SIOAAP – Connessioni a DB AOU SASSARI	279
Tabella 306 – Flussi PICASSO AOU SASSARI	280
Tabella 307 – Flussi PICASSO – Connessioni a DB AOU SASSARI.....	281
Tabella 308 – Flussi Spagic AOU SASSARI.....	281
Tabella 309 – Regole Firewall AOU SASSARI	282
Tabella 310 – Policy di backup AOU SASSARI.....	286
Tabella 311 – Lista componenti CRESSAN.....	288

Tabella 312 – Caratteristiche CRESSAN.....	290
Tabella 313 – Dimensionamento CRESSAN.....	291
Tabella 314 – Composizione storage CRESSAN	291
Tabella 315 – Piano di indirizzamento CRESSAN	292
Tabella 316 – Software installato CRESSAN	294
Tabella 317 – Web Server CRESSAN	294
Tabella 318 – Database server CRESSAN	295
Tabella 319 – DNS CRESSAN.....	296
Tabella 320 – Storage condivisi CRESSAN	296
Tabella 321 – Bilanciamento CRESSAN	298
Tabella 322 – Tipo keepalive CRESSAN	298
Tabella 323 – Tipo persistenza sessione CRESSAN	299
Tabella 324 – Tipologia balancing CRESSAN.....	299
Tabella 325 – Tipo domain enable CRESSAN.....	299
Tabella 326 – Type CRESSAN	299
Tabella 327 – Reverse proxy CRESSAN.....	299
Tabella 328 - Flussi SIOAAP CRESSAN	301
Tabella 329 - Flussi SIOAAP CRESSAN - Connessioni a DB.....	301
Tabella 330 - Flussi PICASSO CRESSAN.....	302
Tabella 331 - Flussi PICASSO - Connessione a DB CRESSAN	302
Tabella 332 – Regole firewall CRESSAN	310
Tabella 333 – Policy di backup CRESSAN.....	314
Tabella 334 – Configurazione ambiente To-Be	318
Tabella 335 - Dimensionamento sito di transito	318
Tabella 336 - Task strategia di migrazione virtual machine	319
Tabella 337 - Task Pre-cutover - Golden Gate.....	320

Tabella 338 - Task Cutover - Golden Gate.....	320
Tabella 339 - Drilldown RMAN	321
Tabella 340 - Prerequisiti migrazione con Oracle Golden Gate	322
Tabella 341 - Primo mock.....	324
Tabella 342 - Test list piattaforma applicativa SISaR	343
Tabella 343 - Task pre-cutover e matrice RACI	345
Tabella 344 - Dettaglio timeline di cutover	347
Tabella 345 - Referenti PSN per la Gestione della Migrazione del Servizio	348
Tabella 346 - Referenti PSN Enabler per la Gestione della Migrazione del Servizio	348

INDICE DELLE FIGURE

Figura 1 - Schema logico ASL1	37
Figura 2 - Autenticazione Pua Comuni.....	53
Figura 3 - Schema logico ASL2	61
Figura 4 - Schema logico ASL3	84
Figura 5 - Schema logico ASL4	108
Figura 6 - Schema logico ASL5	131
Figura 7 - Schema logico ASL6	154
Figura 8 - Schema logico ASL7	176
Figura 9 - Schema logico ASL8	198
Figura 10 - Schema logico ARNAS.....	221
Figura 11 - Schema logico AOU CAGLIARI	246
Figura 12 - Schema logico AOU SASSARI.....	266
Figura 13 - Schema logico CRESSAN	288
Figura 14 - Soluzione di microsegmentazione Cressan - Intra Layer	304
Figura 15 - Soluzione di microsegmentazione Cressan - Extra Layer.....	305

Figura 16 - Applicazioni esposte dai dipartimentali ambiente as-is.	315
Figura 17 - Applicazioni esposte dalle AOU ambiente as-is.	316
Figura 18 - Strategia di migrazione virtual machine	319
Figura 19 - Strategia di Migrazione - Golden Gate	321
Figura 20 - Strategia di Migrazione - Golden Gate – Primo import datai da eseguire con RMAN.	321
Figura 23 - Timeline Pre-cutover - Virtual Machines	344
Figura 24 - Timeline cutover.....	346

STATO DEL DOCUMENTO

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

TITOLO DEL DOCUMENTO		
Descrizione Modifica	Revisione	Data
Prima Emissione	1.0	28/10/2024
Applicazione delle osservazioni pervenute tramite PEC da ARES in data 25/11/2024	2.0	11/12/2024
Applicazione delle osservazioni pervenute tramite PEC da ARES in data 05/02/2025	3.0	29/05/2025
Correzione refusi.	3.1	23/06/2025

Tabella 1 - Informazioni Documento

Autore	
GdL PSN	

Tabella 2 - Autore

Revisione	
PMCA	Federico Ferretti

Tabella 3 - Revisore

Approvazione	
PMCA	Federico Ferretti

Tabella 4 - Approvatore

LISTA DI DISTRIBUZIONE

INTERNA A:

- Funzione Cloud Engineering & Migration
- Funzione Information Security
- Referente Servizio
- Direttore Servizio
- PMCA
- Strutture Tecniche

ESTERNA A:

- Direttore Esecuzione Contrattuale: Dina Assunta Ari
 - Email: dinaassunta.ari@aressardegna.it
- Responsabile Unico Procedimento: Cesare Delussu
 - Email: cesare.delussu@aressardegna.it
- Referente Tecnico: Dina Assunta Ari
 - Email: dinaassunta.ari@aressardegna.it

1 PREMESSA

Il presente documento descrive il Progetto Esecutivo di Dettaglio contenente le specifiche tecniche, le attività e il piano temporale di dettaglio relativi alla migrazione dei **Servizi erogati dalla piattaforma applicativa SISaR** dell'Amministrazione **ARES Sardegna - Azienda Regionale della Salute** (di seguito Amministrazione) nel PSN.

Quanto descritto, è stato redatto in conformità alle richieste dell'Amministrazione, sulla base delle esigenze emerse durante gli incontri tecnici per la raccolta dei requisiti e delle informazioni contenute nel Progetto del Piano dei Fabbisogni e del Piano di Migrazione di Massima ivi contenuto (ID **2023-0000003990570925-PPdF-P1R1**), nonché nel Piano di Migrazione di Dettaglio (ID **2023-0000003990570925-PMD-P1R1**) relativamente alla richiesta di fornitura dei servizi cloud nell'ambito della concessione per la 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.

2 DOCUMENTI DI RIFERIMENTO

Riferimento	Titolo	Documenti consegnati
#1	Piano dei Fabbisogni di Servizio	PSN_Piano dei Fabbisogni_1.0
#2	Progetto del Piano dei Fabbisogni	PSN_Progetto dei Fabbisogni_1.0
#3	Piano di Migrazione di Dettaglio	PSN_Piano di Migrazione di Dettaglio_1.0
#4	Piano di Sicurezza	PSN-SDE-CONV22-001-PianoSicurezza v.1.0 Allegati: PSN - Processo IM v.03 2.C Qualificazione Servizi Cloud 2.B Fornitore Servizio Cloud 2.A Soggetto Infrastruttura Digitale
#5	Piano di Qualità	PSN-SDE-CONV22-002-Piano della Qualità
#6	Piano di Continuità Operativa	PSN-SDE-CONV22-002-Piano di Continuità Operativa ver.1.0

Tabella 5 - Documenti Contrattuali

3 ACRONIMI

La seguente tabella riporta le descrizioni o i significati degli acronimi e delle abbreviazioni presenti nel documento.

Acronimo	Descrizione
ACN	Agenzia per la Cybersicurezza Nazionale
AI	Artificial Intelligence
AO	Azienda Ospedaliera
AOU	Azienda Ospedaliera Universitaria
API	Application Programming Interface
ARES	Azienda Regionale della Salute Sardegna
AREUS	Azienda Regionale per l’Emergenza Urgenza della Sardegna
ARNAS	Azienda di Rilievo Nazionale ed Alta Specializzazione
ASL	Azienda Sanitaria Locale
BI	Business Intelligence
BYOL	Bring Your Own License
CA	Continuità Assistenziale
CaaS	Container as a Service
CAD	Computer Aided Dispatching
CMP	Cloud Management Platform
CO 118	Centrale Operativa 118
CRC	Cyclic Redundancy Check
CRESSAN	Centro Regionale dei Servizi Sanitari della Sardegna
CSP	Cloud Service Provider
CTI	Computer Telephony Integration
CU	Console Unica
CUR	Centrale Unica di Risposta
DAST	Dynamic Application Security Test
DB / DBMS	DataBase / DataBase Management System
DBaaS	DataBase as a Service
DC	Data Center
DWH	Data WareHouse
DR	Disaster Recovery
DTD	Dipartimento per la Trasformazione Digitale
EPS	Events Per Second

Acronimo	Descrizione
EST	Emergenza Sanitaria Territoriale
ETL	Extract Transform and Load
GB	Giga Byte
GCP	Google Cloud Platform
GDPR	General Data Protection Regulation
HA	High Availability
IaaS	Infrastructure as a Service
IAM	Identity and Access Management
IaC	Infrastructure as Code
IT	Information Technology
ITSM	Information Technology Service Management
MDR	Managed Detection and Response
MMG/PLS	Medici di Medicina Generale / Pediatri di Libera Scelta
MPLS	MultiProtocol Label Switching
NAS	Network Attached Storage
NEA 116117	Numero Europeo Armonizzato 116117
NGFW	Next Generation Firewall
NUE 112	Numero Unico Emergenza 112
NVMe	Non-Volatile Memory express
OTT	Over-The-Top
PA	Pubblica Amministrazione
PaaS	Platform as a Service
PMCA	Project Manager di Contratto Adesione
PSAP	Public Safety Answering Point
PNRR	Piano nazionale di Ripresa e Resilienza
PSN	Polo Strategico Nazionale
RAM	Random Access Memory
RMAN	Recovery Manager Oracle
RPO	Recovery Point Objective
RTO	Recovery Time Objective
SAN	Storage Area Network
SCORM	Shareable Content Object Reference Model
SIEM	Security Information and Event Management

Acronimo	Descrizione
SISaR	Sistema Informativo Sanitario integrato Regionale della Sardegna
SO/OS	Sistema Operativo/Operating System
SPC	Sistema Pubblico di Connettività
SSUEM 118	Servizio Sanitario di Urgenza ed Emergenza 118
TB	Tera Byte
TDE	Transparent Data Encryption
UAT	User Acceptance Test
VA/PT	Vulnerability Assesment/Penetration Testing
VCDA	VMware Cloud Director Availability
vCPU	virtual Central Processing Unit
vGB	virtual Giga Byte
VM	Virtual Machine
vNGFW	virtual Next Generation Firewall
VPN	Virtual Private Network
VRF	Virtual Routing and Forwarding
WBT	Web Based Training
WORM	Write Once, Read Many
vWAF	virtual Web Application Firewall

Tabella 6 - Acronimi

4 AMBIENTE TO-BE - PRODUZIONE

4.1 ASL 1 - SASSARI

4.1.1 Architettura

L'architettura applicativa, rappresentata in Figura 1, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud. La stessa implementazione del servizio di database Oracle menzionato sarà utilizzata sia dal tenant ALS 1 di Sassari che dal tenant AO USS, in continuità con l'architettura attualmente in esercizio on-premise. Non è possibile dedicare un DBMS Oracle ad uso esclusivo del tenant AO USS a causa delle seguenti problematiche:

- È necessario stimare e realizzare un intervento per estendere l'interoperabilità anagrafica e adeguare le integrazioni dei sistemi dipartimentali coinvolti con sistemi esterni.
- Si verificherebbe una perdita di univocità dell'ID Paziente dipartimentale nei confronti di sistemi di terze parti, con conseguenti gravi disservizi e rischi di anomalie sui dati.
- I sistemi di terze parti non sono predisposti a ricevere richieste o inviare aggiornamenti di stato a endpoint diversi.
- Le attuali interazioni tramite DBLink richiederebbero una reingegnerizzazione delle integrazioni.
- Non sarebbe possibile effettuare la migrazione di sicurezza inversa con Golden Gate, precludendo un piano di rollback in caso di esito migratorio non conforme alle previsioni.
- La pianificazione della migrazione subirebbe ritardi.

Pertanto, ASL 1 di Sassari e AO USS condivideranno la stessa infrastruttura DBMS Oracle su Exadata Cloud Service, pur disponendo di infrastrutture IaaS Shared HA dedicate.

L'architettura di sicurezza, rappresentata in Figura 1, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 1 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl1, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl1.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl1.

Nel layer di FrontEnd sono presenti due bilanciatori (asl1-lbl1-psn – asl1-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.1.1.1 Schema Logico

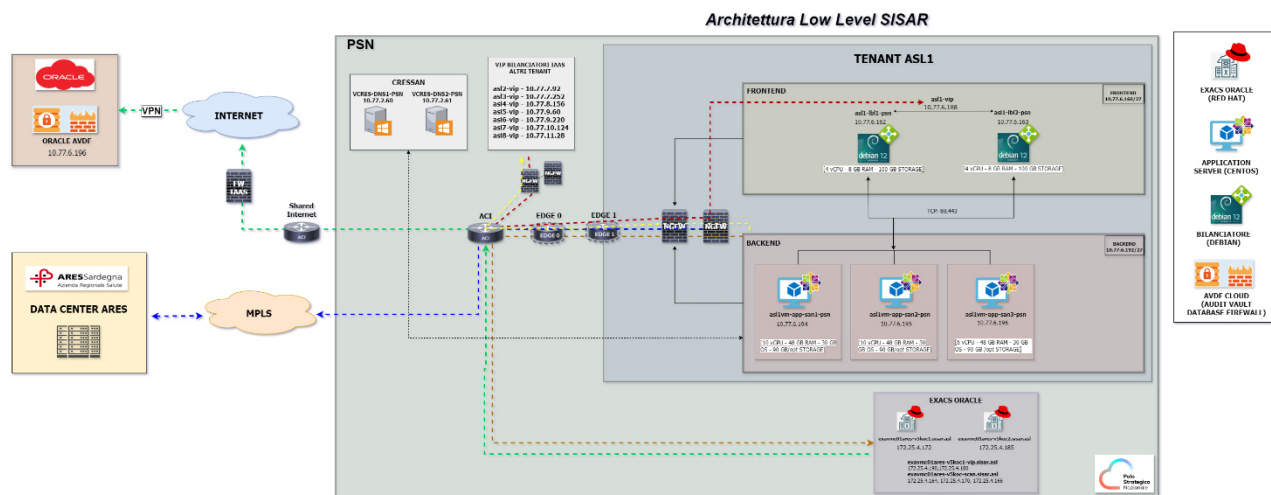


Figura 1 - Schema logico ASL1

4.1.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
as1vm-app-san1-psn	ASL1	Application	Application Server	Virtuale	No
as1vm-app-san2-psn	ASL1	Application	Application Server	Virtuale	No
as1vm-app-san3-psn	ASL1	Application	Application Server	Virtuale	No
as1-vip-psn	ASL1	Presentation	Virtual IP	Virtuale	No
as1-lbl1-psn	ASL1	Presentation	Balancer	Virtuale	No
as1-lbl2-psn	ASL1	Presentation	Balancer	Virtuale	No
N/A	ASL1	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 7 – Lista componenti ASL1

4.1.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.1.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.1.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl1vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl1vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl1vm-app-san3-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl1-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl1-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 8 – Caratteristiche ASL1

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.1.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl1vm-app-san1-psn	10	48	OS 30GB - /opt 90GB	SSD
asl1vm-app-san2-psn	10	48	OS 30GB - /opt 90GB	SSD
asl1vm-app-san3-psn	6	48	OS 30GB - /opt 90GB	SSD
asl1-lbl1-psn	4	8	100	SSD
asl1-lbl2-psn	4	8	100	SSD

Tabella 9 – Dimensionamento ASL1

4.1.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl1vm-app-san1-psn	XFS	Non presente
asl1vm-app-san2-psn	XFS	Non presente
asl1vm-app-san3-psn	XFS	Non presente
asl1-lbl1-psn	XFS	Non presente
asl1-lbl2-psn	XFS	Non presente

Tabella 10 – Composizione storage ASL1

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.1.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC
asl1vm-app-san1-psn	10.77.6.194	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.192/27	N/A
asl1vm-app-san2-psn	10.77.6.195	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.192/27	N/A
asl1vm-app-san3-psn	10.77.6.196	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.192/27	N/A
asl1-vip	10.77.6.188	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.160/27	N/A
asl1-lbl1-psn	10.77.6.162	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.160/27	N/A
asl1-lbl2-psn	10.77.6.163	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.6.160/27	N/A

Tabella 11 – Piano di indirizzamento ASL1

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.1.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl1vm-app-san1-psn	Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181 -----	Servizi Applicativi	NO	ASK DEV	Open Source
	Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_10 -----				
	Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35- asl1 Tomcat version: 8.0.35 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181				

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl1vm-app-san2-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35- aouss Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl1-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl1-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 12 – Software installato ASL1

4.1.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl1vm-app-san1-psn	Tomcat	8	Open Source
asl1vm-app-san2-psn	Tomcat	8	Open Source

Tabella 13 – Web Server ASL1

4.1.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL1PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 14 – Database Server ASL1

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.1.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 15 - Server DNS ASL1

4.1.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
N/A	N/A	N/A	N/A	N/A

Tabella 16 – Storage condivisi ASL1

4.1.2.5 Networking

4.1.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.1.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	soweb- asl1.sisar.asl	http://soweb- asl1.sisar.asl/	asl1vm-app-san1-psn	10.77.6.194:8280
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	spresal- asl1.sisar.asl	http://spresal- asl1.sisar.asl/Spresal	asl1vm-app-san1-psn	10.77.6.194:8380
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	sian- asl1.sisar.asl	spresal-asl1.sisar.asl	asl1vm-app-san1-psn	10.77.6.194:8089
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	sian- asl1.sisar.asl	spresal-asl1.sisar.asl	asl1vm-app-san1-psn	10.77.6.194:8089
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	areas- asl1.sisar.asl	http://areas- asl1.sisar.asl/areas	asl1vm-app-san2-psn	10.77.6.194:8080 10.77.6.194:8180 10.77.6.195:8080 10.77.6.195:8180
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	puacomuni- asl1.sardegna- alute.it	http://puacomuni- asl1.sardegna- alute.it/pua	asl1vm-app-san2-psn	10.77.6.195:8180
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	puacomuni- asl1.sardegna- alute.it	http://puacomuni- asl1.sardegna- alute.it/ras-sp	asl1vm-app-san2-psn	10.77.6.195:8180
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	ml- asl1.sisar.asl	http://ml- asl1.sisar.asl/diagnosiF unzionaleAreas	asl1vm-app-san3-psn	10.77.6.196:8680
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80	ml- asl1ts.sisar.asl	http://ml- asl1ts.sisar.asl/diagnosi FunzionaleAreas	asl1vm-app-san3-psn	10.77.6.196:8090
asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	80		/LBLHealthCheck		localhost:5991

Tabella 17 – Bilanciamento ASL1

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 18 – Tipo keepalive ASL1

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 19 – Tipo persistenza sessione ASL1

Tipologia balancing

Bilanciamento
Least Connection

Tabella 20 – Tipologia balancing ASL1

Tipo Domain Enable

Domain Enable
True

Tabella 21 – Tipo domain Enable ASL1

Type

Type
Adaptive

Tabella 22 – Type ASL1

4.1.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.6.162 10.77.6.163	10.77.6.188	asl1-lbl1-psn asl1-lbl2-psn	ADC_CUPW EB_PUB	ADC CupWeb Pubblico	puacomuni- asl1.sardegna- asalute.it	Adaptive	True	<div>pua- asl1.sisar.asl :80/pua</div> <div>pua- asl1.sisar.asl :80/ras-sp</div>	redirect to LBL priv ASL1

Tabella 23 – Reverse proxy ASL1

4.1.2.5.4 Flussi e Accessibilità

4.1.2.5.4.1 Flussi interni

4.1.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostna me \ DNS destinat ion	IP destination	Protocollo \ tecnologia	Port a	Read \ write	Contenuto flusso
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl8.sisar.asl	N/A	10.77.11.3	TCP	80 443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn	10.77.8.262 10.77.8.263	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA

	asl4vm-app-san2-psn								
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA

Tabella 24 – Flussi SIOAAP ASL1

4.1.2.5.4.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto o flusso
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 25 – Flussi SIOAAP – Connessioni a DB ASL1

4.1.2.5.4.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL1	asl1-lbl1-psn asl1-lbl2-psn	10.77.6.162 10.77.6.163	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Application Server ASL1	asl1vm- app-san1- psn asl1vm- app-san2- psn asl1vm- app-san3- psn	10.77.6.194 10.77.6.195 10.77.6.196	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
----------------------------	---	---	------------	----------------------------------	--------------------------	------------	----	--	----------------

Tabella 26 – Flussi DNS ASL1

4.1.2.5.4.4 Flussi esterni

4.1.2.5.4.5 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Port a	Read \ write	Contenut o flusso
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	cot.aressardeg na.it	cot.aressardeg na.it	93.39.83.53		TCP	443		Integrazio ne con COT
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195 10.77.6.196	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	interoperabilit a.inail.it	interoperabilit a.inail.it	93.147.161.149		TCP	443		PS Inail integrazio ne
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	pddras	pddras	10.39.250.12		TCP	443		PS Inail Integrazio ne
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	cupweb.sisar.a sl	cupweb.sisar.a sl	10.3.66.140		TCP	80 443		E- prescriptio n integrazio ne
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazio ne

areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	protocollo.sisa r.asl	protocollo.sisa r.asl	10.3.66.40		TCP	80 443		Protocollo Integrazio ne
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	vip-picasso- cressan.sisar.a sl	vip-picasso- cressan.sisar.a sl	tutti i nodi		TCP	443		Integrazio ne Picasso (ADT-EDF)

Tabella 27 – Flussi SIOAAP ASL1

4.1.2.5.4.6 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destinatio n	Tipo siste ma ester no (SaaS , on prem ,...)	Proto collo \ tecno logia	Porta	Rea d \ writ e	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc- scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb- scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres- monitorps	vcres- monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 28 – Flussi SIOAAP – Connessioni a DB ASL1

4.1.2.5.4.7 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destinatio n	Hostname \ DNS destinatio n	IP destinatio n	Tipo sistema esterno (SaaS, on prem ,...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker- node- 01.cluster- okd.sisar.a sl	10.3.61.50	areas- asl1.sisar.a sl	areas- asl1.sisar.a sl	10.77.6.18 8		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker- node- 02.cluster- okd.sisar.a sl	10.3.61.51	areas- asl1.sisar.a sl	areas- asl1.sisar.a sl	10.77.6.18 8		TCP	80 443		INTEGRAZI ONE PICASSO

Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl1.sisar.asl	areas-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl1.sisar.asl	spresal-asl1.sisar.asl	10.77.6.188		TCP	80443		INTEGRAZIONE PICASSO

Tabella 29 – Flussi PICASSO ASL1

4.1.2.5.4.8 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 30 – Flussi PICASSO – Connessioni a DB ASL1

4.1.2.5.4.9 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl1vm-esb-san1	10.77.6.196			10.77.6.194			8080	R/W	tipo: http da spagic a WS; flusso: Silus_getreferto

Tabella 31 – Flussi SPAGIC ASL1

4.1.2.5.4.10 Accessi esterni/interni

Endpoint pubblico / esterno	IP pubblico / esterno	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://soweb-asl1.sisar.asl/	10.77.6.188	asl1vm-app-san1-psn	10.77.6.194	HTTP	8280		No
http://spresal-asl1.sisar.asl/	10.77.6.188	asl1vm-app-san1-psn	10.77.6.194	HTTP	8380		No
http://sian-asl1.sisar.asl/	10.77.6.188	asl1vm-app-san1-psn	10.77.6.194	HTTP	8089		No
http://areas-asl1.sisar.asl/areas	10.77.6.188	asl1vm-app-san1-psn asl2vm-app-san2-psn	10.77.6.194 10.77.6.195	HTTP	8080 8180		No
http://puacomuni-asl1.sardegna.sute.it	10.77.6.188	asl2vm-app-san1-psn	10.77.6.195	HTTPS	8180		Si
http://ml-asl1.sisar.asl	10.77.6.188	asl1vm-app-san1-psn	10.77.6.196	HTTP	8680		No

Tabella 32 – Accessi esterni/interni ASL1

4.1.2.6 Sicurezza

4.1.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono di seguito descritti i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML:

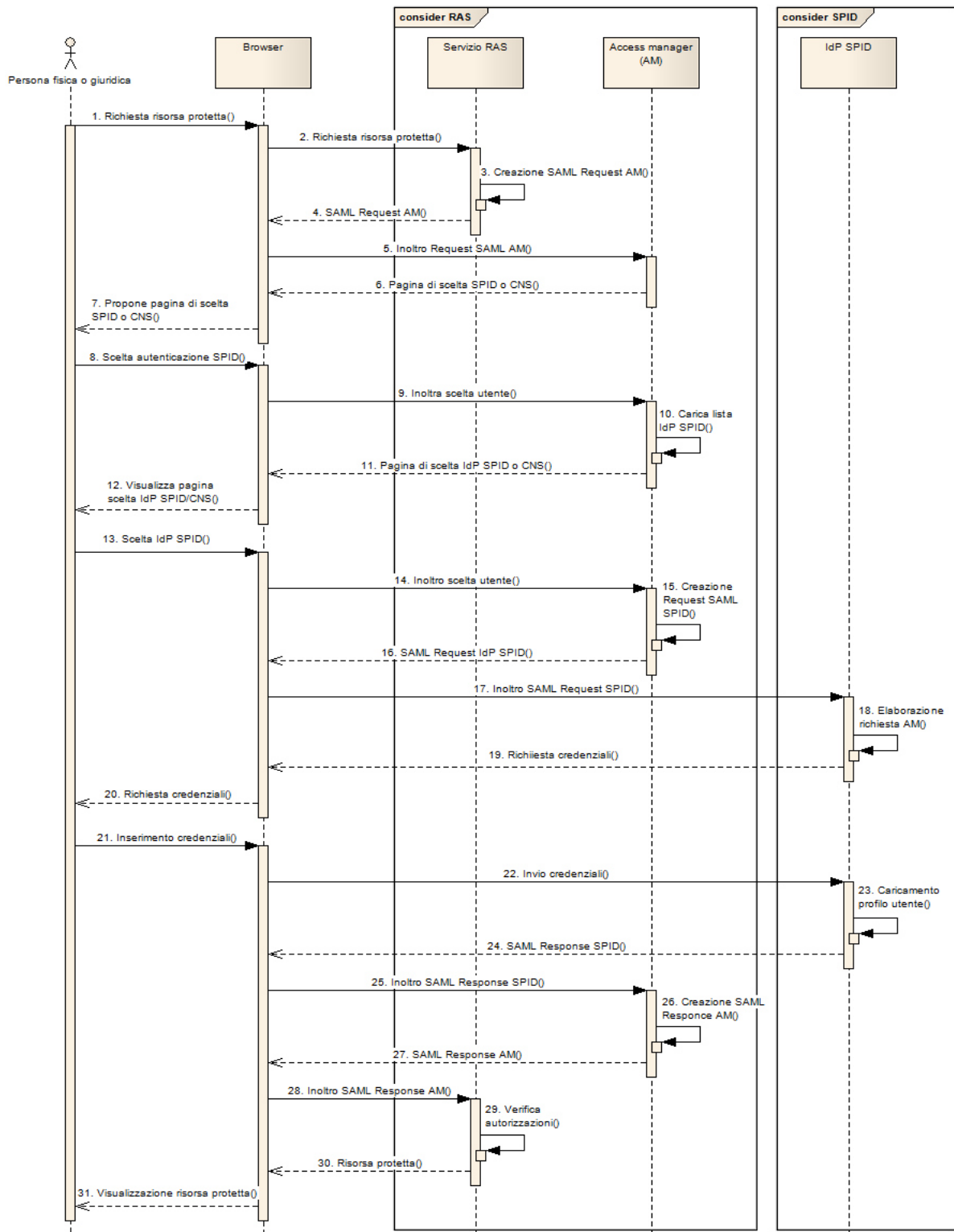


Figura 2 - Autenticazione Pua Comuni

4.1.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegناسalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.1.2.6.3 Regole Firewall

Hostname sorgente	Rete/IP Sorgente	Hostname destinazione	Rete/IP Destinazione	Protocollo	TCP/UDP	Porte	Note
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail integrazione
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E-prescription integr.
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn	10.77.6.194 10.77.6.195	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

asl1vm-app-san2-psn							
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		TBD		TCP	1521	Flussi Applicativi SIOAAP - database sioaap
asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF)
asl1vm-app-san1-psn	10.77.6.194	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL1 to DNS CRESSAN
asl1vm-app-san2-psn	10.77.6.195	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL1 to DNS CRESSAN
asl1vm-app-san1-psn	10.77.6.196	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL1 to DNS CRESSAN
asl1-lbl1-psn	10.77.6.162	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL1 to DNS CRESSAN
asl1-lbl2-psn	10.77.6.163	VCRES-DNS1-PSN	10.77.2.60		TCP/UDP	53	from ASL1 to DNS CRESSAN

		VCRES-DNS2-PSN	10.77.2.61				
--	--	----------------	------------	--	--	--	--

Tabella 33 – Regole Firewall ASL1

4.1.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.1.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e

assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl1vm-app-san1-psn	10.77.6.194	Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl1vm-app-san2-psn	10.77.6.195	Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl1vm-app-san1-psn	10.77.6.196	Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl1-lbl1-psn	10.77.6.162	Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl1-lbl2-psn	10.77.6.163	Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 34 – Policy di backup ASL1

4.1.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di

migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.2 ASL 2 – OLBIA

4.2.1 Architettura

L'architettura applicativa, rappresentata in Figura 3, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 3, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 2 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl2, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl2.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl2.

Nel layer di FrontEnd sono presenti due bilanciatori (asl2-lbl1-psn asl2-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.2.1.1 Schema Logico

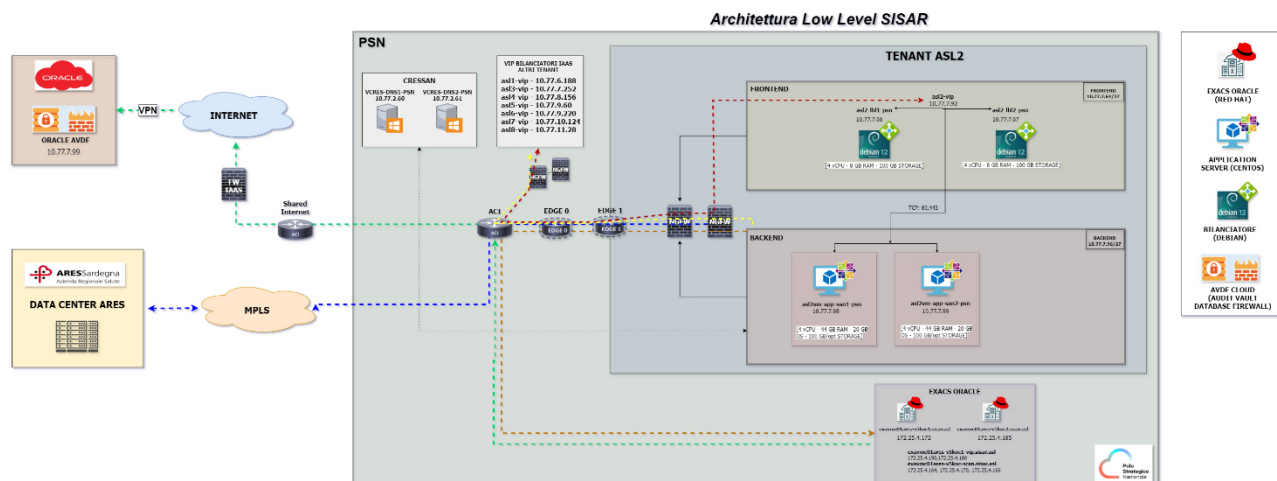


Figura 3 - Schema logico ASL2

4.2.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl2vm-app-san1-psn	ASL2	Application	Application Server	Virtuale	No
asl2vm-app-san2-psn	ASL2	Application	Application Server	Virtuale	No
asl2-vip-psn	ASL2	Presentation	Virtual IP	Virtuale	No
asl2-lbl1-psn	ASL2	Presentation	Balancer	Virtuale	No
asl2-lbl2-psn	ASL2	Presentation	Balancer	Virtuale	No
N/A	ASL2	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 35 – Lista componenti ASL2

4.2.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.2.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.2.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl2vm-app-san1-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl2vm-app-san2-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl2-lbl1-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	Debian	12 bookworm
asl2-lbl2-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 36 – Caratteristiche ASL2

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.2.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl2vm-app-san1-psn	4	44	OS 20GB - /opt 100GB	SSD
asl2vm-app-san2-psn	4	44	OS 20GB - /opt 100GB	SSD
asl2-lbl1-psn	4	8	100	SSD
asl2-lbl2-psn	4	8	100	SSD

Tabella 37 – Dimensionamento ASL2

4.2.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl2vm-app-san1-psn	XFS	Non presente
asl2vm-app-san2-psn	XFS	Non presente
asl2-lbl1-psn	XFS	Non presente
asl2-lbl2-psn	XFS	Non presente

Tabella 38 – Composizione storage ASL2

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.2.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl2vm-app-san1-psn	10.77.7.98	PSN Industry Standard HA – Ambiente ASL02 - TGU servizio PSN02838228	10.77.7.96/27	N/A
asl2vm-app-san2-psn	10.77.7.99	PSN Industry Standard HA – Ambiente ASL02 - TGU servizio PSN02838228	10.77.7.96/27	N/A
asl2-vip	10.77.7.92	PSN Industry Standard HA – Ambiente ASL02 - TGU servizio PSN02838228	10.77.7.64/27	N/A
asl2-lbl1-psn	10.77.7.66	PSN Industry Standard HA – Ambiente ASL02 - TGU servizio PSN02838228	10.77.7.64/27	N/A
asl2-lbl2-psn	10.77.7.67	PSN Industry Standard HA – Ambiente ASL02 - TGU servizio PSN02838228	10.77.7.64/27	N/A

Tabella 39 – Piano di indirizzamento ASL2

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.2.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl2vm-app-san1-psn	<p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl2vm-app-san2-psn	<p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25 Tomcat version: Unknown JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl2-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl2-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 40 – Software installato

4.2.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl2vm-app-san1-psn	Tomcat	8	Open Source
asl2vm-app-san2-psn	Tomcat	8	Open Source

Tabella 41 – Web server ASL2

4.2.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL2PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 42 – Database Server ASL2

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.2.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 43 - Server DNS ASL2

4.2.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 44 – Storage condivisi ASL2

4.2.2.5 Networking

4.2.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.2.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://areas-asl2.sisar.asl/areas	http://areas-asl2.sisar.asl/areas	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98:8080 10.77.7.99:8080 10.77.7.99:8180
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://integasl2.sisar.asl/areas	http://integasl2.sisar.asl/demone	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98:8080 10.77.7.99:8080
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://ml-asl2.sisar.asl/	http://ml-asl2.sisar.asl/diagnosiFunzionaleAreas	asl2vm-app-san2-psn	10.77.7.98:8580
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://puacomuni-asl2.sardegna salute.it	http://puacomuni-asl2.sardegna salute.it/pua	asl2vm-app-san1-psn	10.77.7.98:8180
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://puacomuni-asl2.sardegna salute.it	http://puacomuni-asl2.sardegna salute.it/pua	asl2vm-app-san1-psn	10.77.7.98:8180
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://puacomuni-asl2.sardegna salute.it	http://puacomuni-asl2.sardegna salute.it/ras-sp	asl2vm-app-san1-psn	10.77.7.98:8180
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://puacomuni-asl2.sardegna salute.it	http://puacomuni-asl2.sardegna salute.it/ras-sp	asl2vm-app-san1-psn	10.77.7.98:8180
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://sian-asl2.sisar.asl/	/	asl2vm-app-san1-psn	10.77.7.98:8089
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://sian-asl2.sisar.asl/	/SianWUI	asl2vm-app-san1-psn	10.250.62.54:8089
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://sian-asl2.sisar.asl/	/SianWS	asl2vm-app-san1-psn	10.250.62.54:8089

asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://soweb- asl2.sisar.asl/		asl2vm-app-san1- psn	10.77.7.98:8280
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://spresal- asl2.sisar.asl/	http://spresal- asl2.sisar.asl/Spres al	asl2vm-app-san2- psn	10.77.7.99:8380
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	http://spresal- asl2.sisar.asl/		asl2vm-app-san2- psn	10.250.62.56:8380
asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	80	healthcheck	/LBLHealthCheck		

Tabella 45 – Bilanciamento ASL2

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 46 – Tipo keepalive ASL2

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 47 – Tipo persistenza sessione ASL2

Tipologia balancing

Bilanciamento
Least Connection

Tabella 48 – Tipologia balancing ASL2

Tipo Domain Enable

Domain Enable
True

Tabella 49 – Tipo domain Enable ASL2

Type

Type
Adaptive

Tabella 50 – Type ASL2

4.2.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.7.66 10.77.7.67	10.77.7.92	asl2-lbl1-psn asl2-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl2.sardegna salute.it	Adaptative	true	<p>puasasl2.sisar.asl:80/pua</p> <p>puasasl2.sisar.asl:80/ras-sp</p>	<p>redirect to LBL priv ASL2</p>

Tabella 51 – Reverse proxy ASL2

4.2.2.5.4 Flussi e Accessibilità

4.2.2.5.4.1 Flussi interni

4.2.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-	10.77.7.98 10.77.7.99	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA

	app-san2- psn								
areas- asl2.sisar.asl	asl2vm- app-san1- psn asl2vm- app-san2- psn	10.77.7.98 10.77.7.99	areas- asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas- asl2.sisar.asl	asl2vm- app-san1- psn asl2vm- app-san2- psn	10.77.7.98 10.77.7.99	areas- asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas- asl2.sisar.asl	asl2vm- app-san1- psn asl2vm- app-san2- psn	10.77.7.98 10.77.7.99	areas- asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas- asl2.sisar.asl	asl2vm- app-san1- psn asl2vm- app-san2- psn	10.77.7.98 10.77.7.99	areas- asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl1.sisar.asl	asl1vm- app-san1- psn asl1vm- app-san2- psn	10.77.6.194 10.77.6.195	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl3.sisar.asl	asl3vm- app-san1- psn asl3vm- app-san2- psn	10.77.8.2 10.77.8.3	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl4.sisar.asl	asl4vm- app-san1- psn asl4vm- app-san2- psn	10.77.8.262 10.77.8.263	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl5.sisar.asl	asl5vm- app-san1- psn asl5vm- app-san2- psn	10.77.9.66 10.77.9.66	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl6.sisar.asl	asl6vm- app-san1- psn asl6vm- app-san2- psn	10.77.9.226 10.77.9.227	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm-	10.77.10.130 10.77.10.131	areas- asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA

	app-san2-psn								
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA

Tabella 52 – Flussi SIOAPP ASL2

4.2.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 53 – Flussi SIOAAP – Connessioni a DB ASL2

4.2.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL2	asl2-lbl1-psn asl2-lbl2-psn	10.77.7.66 10.77.7.67	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server ASL2	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 54 – Flussi DNS ASL2

4.2.2.5.4.2 Flussi esterni

4.2.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	cot.aressardeгна.it	cot.aressardeгна.it	93.39.83.53		TCP	443		Integrazione con COT
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	interoperabilita.inail.it	interoperabilita.inail.it	93.147.161.149		TCP	443		PS Inail integrazione
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80443		E-prescription integrazione
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80443		EDF integrazione
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80443		Protocollo Integrazione

areas- asl2.sisar.asl	asl2vm- app-san1- psn asl2vm- app-san2- psn	10.77.7.98 10.77.7.99	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integrazio ne Picasso (ADT- EDF)
--------------------------	--	--------------------------	-----------------------------------	-----------------------------------	--------------	--	-----	-----	--	---

Tabella 55 – Flussi SIOAPP ASL2

4.2.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destinatio n	Tipo sistema esterno (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Porta	Read \ write	Contenut o flusso
Oracle ExaCS	TBD		db_link AMC	cluamc- scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb- scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres- monitorps	vcres- monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 56 – Flussi SIOAAP – Connessioni a DB ASL2

4.2.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Porta	Read \ write	Contenut o flusso
Worker Node Picasso	worker-node- 01.cluster- okd.sisar.asl	10.3.61.50	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 02.cluster- okd.sisar.asl	10.3.61.51	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 03.cluster- okd.sisar.asl	10.3.61.52	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 04.cluster- okd.sisar.asl	10.3.61.53	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 05.cluster- okd.sisar.asl	10.3.61.54	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 06.cluster- okd.sisar.asl	10.3.61.55	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 07.cluster- okd.sisar.asl	10.3.61.56	areas- asl2.sisar.asl	areas- asl2.sisar.asl	10.77.7.92		TCP	80 443		INTEGRAZI ONE PICASSO

Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl2.sisar.asl	areas-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl2.sisar.asl	areas-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl2.sisar.asl	spresal-asl2.sisar.asl	10.77.7.92		TCP	80443		INTEGRAZIONE PICASSO

Tabella 57 – Flussi Picasso

4.2.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 58 – Flussi PICASSO – Connessioni a DB ASL2

4.2.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: Silus_getreferto
	asl2vm-app-san1-psn	10.77.7.98						5050	R/W	servizio http esposto da spagic all'oe - PrintEtichettaEliot
	asl2vm-app-san2-psn	10.77.7.99						5050	R/W	servizio http esposto da spagic all'oe - PrintEtichettaEliot
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: PrintEtichettaEliot
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: CambioStato
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: CambioStatoDettaglio
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: Olbia_PS_to_RAD_Noema
	asl2vm-esb-san1				10.77.7.99			8180	R/W	tipo: http da spagic a WS; flusso: OE_TrasfusionaleReperisciRisultatiHL7

Tabella 59 – Flussi SPAGIC ASL2

4.2.2.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-asl2.sisar.asl/areas	10.77.7.92	Asl2vm-app-san1 Asl2vm-app-san2	10.77.7.98 10.77.7.99	HTTP	8080 8180		no
http://integasl2.sisar.asl/areas	10.77.7.92	Asl2vm-app-san1 Asl2vm-app-san2	10.77.7.98 10.77.7.99	HTTP	8080		no
http://ml-asl2.sisar.asl/	10.77.7.92	Asl2vm-app-san1	10.77.7.98	HTTP	8580		no
http://puacomuni-asl2.sardegناسalute.it	10.77.7.92	Asl2vm-app-san1	10.77.7.98	HTTPS	8180		si
http://sian-asl2.sisar.asl/	10.77.7.92	Asl2vm-app-san1	10.77.7.98	HTTP	8089		no
http://soweb-asl2.sisar.asl/	10.77.7.92	Asl2vm-app-san1	10.77.7.98	HTTP	8280		no
http://spresal-asl2.sisar.asl/	10.77.7.92	Asl2vm-app-san2	10.77.7.99	HTTP	8380		no

Tabella 60 – Accessi esterni/interni ASL2

4.2.2.6 Sicurezza

4.2.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.2.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegناسalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.2.2.6.3 Regole Firewall

Hostname sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail integrazione
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E-prescription integr.
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		Da definire		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
	Da definire		10.3.67.167 10.3.67.168 10.3.67.169		TCP	1521	Flussi Applicativi SIOAAP - db_link AMC (non presente in doc SardegnaIT)
	Da definire		10.3.69.118 10.3.69.119 10.3.69.120		TCP	1521	Flussi Applicativi SIOAAP - db_link CUPWEB (non presente in doc SardegnaIT)
asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99		10.3.61.9				
asl2vm-app-san1-psn	10.77.7.98	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL2 to DNS CRESSAN
asl2vm-app-san2-psn	10.77.7.99	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL2 to DNS CRESSAN
asl2-lbl1-psn	10.77.7.66	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL2 to DNS CRESSAN
asl2-lbl2-psn	10.77.7.67	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL2 to DNS CRESSAN

Tabella 61 – Regole Firewall ASL2

4.2.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.2.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl2vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl2vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl2-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl2-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 62 – Policy di backup ASL2

4.2.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.3 ASL 3 – NUORO

4.3.1 Architettura

L'architettura applicativa, rappresentata in Figura 4, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 4, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control.

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 3 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl3, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl3.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl3.

Nel layer di FrontEnd sono presenti due bilanciatori (asl3-lbl1-psn - asl3-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.3.1.1 Schema Logico

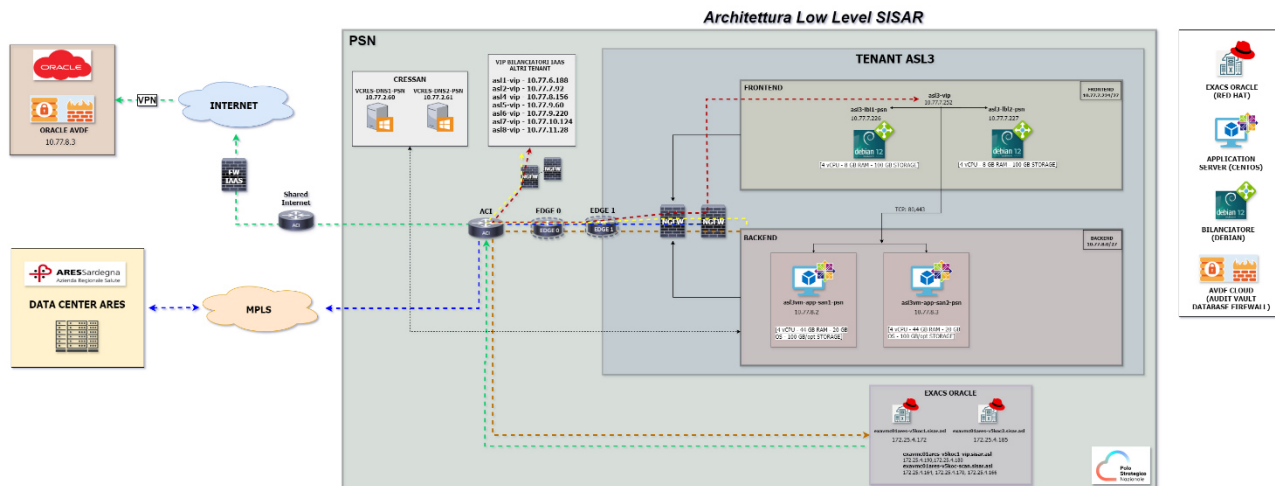


Figura 4 - Schema logico ASL3

4.3.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl3vm-app-san1-psn	ASL3	Application	Application Server	Virtuale	No
asl3vm-app-san2-psn	ASL3	Application	Application Server	Virtuale	No
asl3-vip-psn	ASL3	Presentation	Virtual IP	Virtuale	No
asl3-lbl1-psn	ASL3	Presentation	Balancer	Virtuale	No
asl3-lbl2-psn	ASL3	Presentation	Balancer	Virtuale	No
N/A	ASL3	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 63 – Lista componenti ASL3

4.3.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.3.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.3.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl3vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl3vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl3-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl3-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 64 – Caratteristiche ASL3

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.3.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl3vm-app-san1-psn	4	44	OS 20GB - /opt 100GB	SSD
asl3vm-app-san2-psn	4	44	OS 20GB - /opt 100GB	SSD

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl3-lbl1-psn	4	8	100	SSD
asl3-lbl2-psn	4	8	100	SSD

Tabella 65 – Dimensionamento ASL3

4.3.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl3vm-app-san1-psn	XFS	Non presente
asl3vm-app-san2-psn	XFS	Non presente
asl3-lbl1-psn	XFS	Non presente
asl3-lbl2-psn	XFS	Non presente

Tabella 66 – Composizione storage ASL3

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.3.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl3vm-app-san1-psn	10.77.8.2	PSN Industry Standard HA – Ambiente ASL03 - TGU servizio PSN02838254	10.77.8.0/27	N/A
asl3vm-app-san2-psn	10.77.8.3	PSN Industry Standard HA – Ambiente ASL03 - TGU servizio PSN02838254	10.77.8.0/27	N/A
asl3-vip	10.77.7.252	PSN Industry Standard HA – Ambiente ASL03 - TGU servizio PSN02838254	10.77.7.224/27	N/A
asl3-lbl1-psn	10.77.7.226	PSN Industry Standard HA – Ambiente ASL03 - TGU servizio PSN02838254	10.77.7.224/27	N/A

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl3-lbl2-psn	10.77.7.227	PSN Industry Standard HA – Ambiente ASL03 - TGU servizio PSN02838254	10.77.7.224/27	N/A

Tabella 67 – Piano di indirizzamento ASL3

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.3.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl3vm-app-san1-psn	<p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25 Tomcat version: 5.5.25 JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p>	Servizi Applicativi	NO	ASK DEV	Open Source

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl3vm-app-san2-psn	<p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl3-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl3-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 68 – Software installato ASL3

4.3.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl3vm-app-san1-psn	Tomcat	8	Open Source
asl3vm-app-san2-psn	Tomcat	8	Open Source

Tabella 69 – Web server ASL3

4.3.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL3PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 70 – Database server ASL3

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.3.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 71 - Server DNS ASL3

4.3.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 72 – Storage condivisi ASL3

4.3.2.5 Networking

4.3.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.3.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	areas-asl3.sisar.asl	http://areas-asl3.sisar.asl/areas	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2:8080 10.77.8.3:8080 10.77.8.3:8180
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	eliot-asl3.sisar.asl	http://eliot-asl3.sisar.asl/WDOEliot	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2:8589 10.77.8.3:8589
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	eliot-asl3test.sisar.asl	http://eliot-asl3test.sisar.asl/WDOEliot	asl3vm-app-san1-psn	10.77.8.2:8086
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	ml-asl3.sisar.asl	http://ml-asl3.sisar.asl/diagnosiFunzionaleAreas	asl3vm-app-san1-psn	10.77.8.2:8580
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	puacomuni- asl3.sardegna salute.it		asl3vm-app-san1-psn	10.77.8.2:8180
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	spresal-asl3.sisar.asl	http://spresal-asl3.sisar.asl/Spresal	asl3vm-app-san1-psn	10.77.8.2:8380
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	sian-asl3.sisar.asl	http://sian-asl3.sisar.asl/SianWUI	asl3vm-app-san2-psn	10.77.8.3:8089
asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	80	soweb-asl3.sisar.asl		asl3vm-app-san2-psn	10.77.8.3:8280
asl3-lbl1-psn asl3-lbl2-psn	10.77.6.162 10.77.6.163	80		/LBLHealthCheck		localhost:5991

Tabella 73 – Bilanciamento ASL3

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 74 – Tipo keepalive ASL3

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 75 – Tipo persistenza sessione ASL3

Tipologia balancing

Bilanciamento
Least Connection

Tabella 76 – Tipologia balancing ASL3

Tipo Domain Enable

Domain Enable
True

Tabella 77 – Tipo domain Enable ASL3

Type

Type
Adaptive

Tabella 78 – Type ASL3

4.3.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.7.226 10.77.7.227	10.77.7.25 2	asl3-lbl1-psn asl3-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl3.sardegna salute.it	Adaptative	true	pua- asl3.sisar.asl:80/pua	redirect to LBL priv ASL3
								pua- asl3.sisar.asl:80/ras-sp	

Tabella 79 – Reverse Proxy ASL3

4.3.2.5.4 Flussi e Accessibilità

4.3.2.5.4.1 Flussi interni

4.3.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn	10.77.8.262 10.77.8.263	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA

	asl4vm-app-san2-psn								
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA

Tabella 80 – Flussi SIOAAP ASL3

4.3.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 81 – Flussi SIOAAP – Connessioni a DB ASL3

4.3.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL3	asl3-lbl1-psn asl3-lbl2-psn	10.77.7.226 10.77.7.227	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server ASL3	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 82 – Flussi DNS ASL3

4.3.2.5.4.2 Flussi esterni

4.3.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integrazione con COT
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	interoperabilita.inail.it	interoperabilita.inail.it	93.147.161.149		TCP	443		PS Inail integrazione
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-	10.77.8.2 10.77.8.3	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione

	app-san2-psn									
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80443		E-prescription integrazione
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80443		EDF integrazione
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80443		Protocollo Integrazione
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	vip-picasso-cressan.sisar.asl	vip-picasso-cressan.sisar.asl	tutti i nodi		TCP	443		Integrazione Picasso (ADT-EDF)

Tabella 83 – Flussi SIOAAP ASL3

4.3.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto o flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	tutti i nodi EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	tutti i nodi EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 84 – Flussi SIOAAP – Connessioni a DB ASL3

4.3.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
----------------	-----------------------	-----------	---------------------	----------------------------	----------------	---	-------------------------	-------	--------------	------------------

Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl3.sisar.asl	areas-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl3.sisar.asl	spresal-asl3.sisar.asl	10.77.7.252		TCP	80443		INTEGRAZIONE PICASSO

Tabella 85 – Flussi PICASSO ASL3

4.3.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
---------------------	--------------------------------------	------------	--------------	-----	----------------	--	-----	------	--	----------------------

Tabella 86 – Flussi PICASSO – Connessioni a DB ASL3

4.3.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl3vm-app-san1-psn	10.77.8.2						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl3vm-app-san2-psn	10.77.8.3						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot

Tabella 87 – Flussi SPAGIC ASL3

4.3.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-asl3.sisar.asl/areas	10.77.7.252	Asl3vm-app-san1 Asl3vm-app-san2	10.77.8.2 10.77.8.3	8080 8180	HTTP		no
http://eliot-asl3.sisar.asl	10.77.7.252	Asl3vm-app-san1 Asl3vm-app-san2	10.77.8.2 10.77.8.3	8589	HTTP		no
http://eliot-asl3test.sisar.asl	10.77.7.252	Asl3vm-app-san1	10.77.8.2	8086	HTTP		no
http://ml-asl3.sisar.asl/	10.77.7.252	Asl3vm-app-san1	10.77.8.2	8580	HTTP		no
http://puacomuni-asl3.sardegnaalute.it	10.77.7.252	Asl3vm-app-san1	10.77.8.2	8180	HTTPS		si
http://spresal-asl3.sisar.asl/	10.77.7.252	Asl3vm-app-san1	10.77.8.2	8380	HTTP		no
http://sian-asl3.sisar.asl/	10.77.7.252	Asl3vm-app-san2	10.77.8.3	8089	HTTP		no
http://soweb-asl3.sisar.asl/	10.77.7.252	Asl3vm-app-san2	10.77.8.3	8280	HTTP		no

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://eliot.aslnuoro.it	10.77.7.252	Asl3vm-app-san1 Asl3vm-app-san2	10.77.8.2 10.77.8.3	8590	HTTP		no

Tabella 88 – Accessi esterni/interni ASL3

4.3.2.6 Sicurezza

4.3.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.3.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegna salute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui proprio dispositivi.

4.3.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP -MD. LEG. vs INPS
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E- prescription integr.
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl3vm-app- san1-psn asl3vm-app- san2-psn	10.77.8.2 10.77.8.3		10.160.152.139 10.160.152.139 10.160.152.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.160.152.139 10.160.152.139 10.160.152.141		10.3.67.167 10.3.67.168 10.3.67.169		TCP	1521	Flussi Applicativi SIOAAP - db_link AMC (non presente in doc SardegnaIT)
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.160.152.139 10.160.152.139 10.160.152.141		10.3.69.118 10.3.69.119 10.3.69.120		TCP	1521	Flussi Applicativi SIOAAP - db_link CUPWEB (non presente in doc SardegnaIT)
asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF) (non presente in doc SardegnaIT)
asl3vm-app-san1-psn	10.77.8.2		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL3 to DNS CRESSAN
asl3vm-app-san2-psn	10.77.8.3		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL3 to DNS CRESSAN
asl3-lbl1-psn	10.77.7.226		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL3 to DNS CRESSAN
asl3-lbl2-psn	10.77.7.227		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL3 to DNS CRESSAN

Tabella 89 – Regole firewall ASL3

4.3.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.3.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico

repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
- WORM Protection:
 - Funzionalità della tecnologia di riferimento (Commvault) di WORM (Write Only Read Multiple) che si integra con le medesime funzionalità sullo storage di riferimento del repository;
 - La tecnologia di riferimento (Commvault) blocca i dati di backup da modifiche casuali non autorizzate e previene la modifica o l'eliminazione dei dati di backup intenzionale (I dati di backup saranno cancellati solo quando saranno state raggiunte le retention applicate);
 - Nessun amministratore del backup potrà cancellare i dati di backup non scaduti;
 - La tecnologia di riferimento (Commvault) convalida l'integrità dei dati durante il backup e durante le operazioni di copia dei dati. Quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul client di origine e

archiviati con il backup. Quando si copiano i dati, le firme (checksum CRC) vengono utilizzate per convalidare i blocchi di dati durante l'operazione di copia.

- **Ransomware Protection:**

- Funzionalità Commvault di Ransomware protection;
- I dati di backup sono bloccati e possono essere modificati solo dai processi della tecnologia di riferimento (Commvault);
- Qualsiasi ransomware, applicazione o utente che tenti di eliminare, o modificare i dati di backup dal Media Agent (unico server che può accedere allo storage) riceverà una segnalazione di errore (catastrophic error dallo stack I/O del SO) a meno che non si tratti di un processo della tecnologia di riferimento (Commvault) autorizzato (modalità like SE-Linux).

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl3vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl3vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl3-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl3-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 90 – Policy di backup ASL3

4.3.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.4 ASL 4 – LANUSEI

4.4.1 Architettura

L'architettura applicativa, rappresentata in Figura 5, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 5, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 4 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl4, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl4.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl4.

Nel layer di FrontEnd sono presenti due bilanciatori (asl4-lbl1-psn – asl4-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.4.1.1 Schema Logico

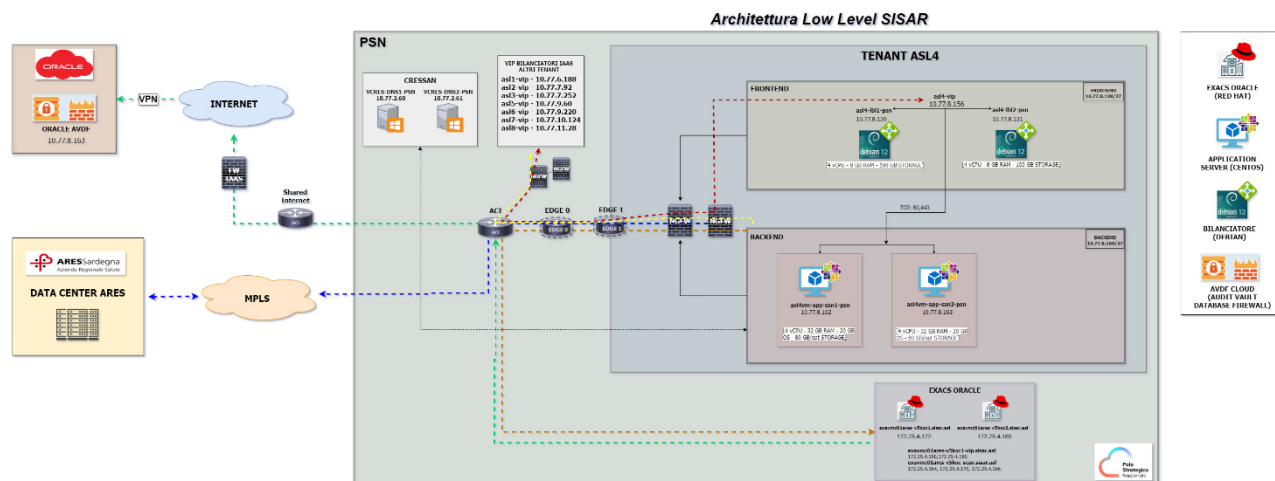


Figura 5 - Schema logico ASL4

4.4.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl4vm-app-san1-psn	ASL4	Application	Application Server	Virtuale	No
asl4vm-app-san2-psn	ASL4	Application	Application Server	Virtuale	No
asl4-vip-psn	ASL4	Presentation	Virtual IP	Virtuale	No
asl4-lbl1-psn	ASL4	Presentation	Balancer	Virtuale	No
asl4-lbl2-psn	ASL4	Presentation	Balancer	Virtuale	No
N/A	ASL4	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 91 – Lista componenti ASL4

4.4.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.4.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.4.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl4vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl4vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl4-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl4-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 92 – Caratteristiche ASL4

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.4.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl4vm-app-san1-psn	4	32	OS 20GB - /opt 80GB	SSD
asl4vm-app-san2-psn	4	32	OS 20GB - /opt 80GB	SSD
asl4-lbl1-psn	4	8	100	SSD
asl4-lbl2-psn	4	8	100	SSD

Tabella 93 – Dimensionamento ASL4

4.4.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl4vm-app-san1-psn	XFS	Non presente
asl4vm-app-san2-psn	XFS	Non presente
asl4-lbl1-psn	XFS	Non presente
asl4-lbl2-psn	XFS	Non presente

Tabella 94 – Composizione storage ASL4

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.4.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl4vm-app-san1-psn	10.77.8.262	PSN Industry Standard HA – Ambiente ASL04 - TGU servizio PSN02838316	10.77.8.260/27	N/A
asl4vm-app-san2-psn	10.77.8.263	PSN Industry Standard HA – Ambiente ASL04 - TGU servizio PSN02838316	10.77.8.260/27	N/A
asl4-vip	10.77.8.256	PSN Industry Standard HA – Ambiente ASL04 - TGU servizio PSN02838316	10.77.8.228/27	N/A
asl4-lbl1-psn	10.77.8.230	PSN Industry Standard HA – Ambiente ASL04 - TGU servizio PSN02838316	10.77.8.228/27	N/A
asl4-lbl2-psn	10.77.8.231	PSN Industry Standard HA – Ambiente ASL04 - TGU servizio PSN02838316	10.77.8.228/27	N/A

Tabella 95 – Piano di indirizzamento ASL4

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.4.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl4vm-app-san1-psn	<p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl4vm-app-san2-psn	<p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25 Tomcat version: Unknown JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl4-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl4-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 96 – Software installato ASL4

4.4.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl4vm-app-san1-psn	Tomcat	8	Open Source
asl4vm-app-san2-psn	Tomcat	8	Open Source

Tabella 97 – Web server ASL4

4.4.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL4PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 98 – Database server ASL4

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.4.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 99 - Server DNS ASL4

4.4.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 100 – Storage condivisi ASL4

4.4.2.5 Networking

4.4.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.4.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	areas-asl4.sisar.asl	http://areas-asl4.sisar.asl/areas	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262:8080 10.77.8.263:8080 10.77.8.263:8180
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	ml-asl4.sisar.asl	http://ml-asl4.sisar.asl/diagnosiFunzionaleAreas	asl4vm-app-san1-psn	10.77.8.262:8580
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	puacomuni-asl4.sardegnaalute.it		asl4vm-app-san1-psn	10.77.8.262:8180
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	sian-asl4.sisar.asl	http://sian-asl4.sisar.asl/SianWUI	asl4vm-app-san1-psn	10.77.8.262:8089
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	smxint-areas-asl4.sisar.asl	http://smxint-areas-asl4.sisar.asl/demone/	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262:8080 10.77.8.263:8080
asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	80	soweb-asl4.sisar.asl		asl4vm-app-san1-psn	10.77.8.262:8280
asl4-lbl1-psn	10.77.8.230 10.77.8.231	80	spresal-asl4.sisar.asl	http://spresal-asl4.sisar.asl/Spresal	asl4vm-app-san2-psn	10.77.8.263:8380

asl4-lbl2-psn						
asl4-lbl1-psn	10.77.8.230	80		/LBLHealthCheck		localhost:5991
asl4-lbl2-psn	10.77.8.231					

Tabella 101 – Bilanciamento ASL4

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 102 – Tipo keepalive ASL4

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 103 – Tipo persistenza sessione ASL4

Tipologia balancing

Bilanciamento
Least Connection

Tabella 104 – Tipologia balancing ASL4

Tipo Domain Enable

Domain Enable
True

Tabella 105 – Tipo domain Enable ASL4

Type

Type
Adaptive

Tabella 106 – Type ASL4

4.4.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note	Note
10.77.8.230 10.77.8.231	10.77.8.256	asl4-lbl1-psn asl4-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl4.sardegna salute.it	Adaptative	true	<p>pu-a-slar4.sisar.asl:80/pua</p> <p>pu-a-slar4.sisar.asl:80/ras-sp</p>	/pu-a	redirect to LBL priv ASL4

Tabella 107 – Reverse proxy ASL4

4.4.2.5.4 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-asl4.sisar.asl/areas	10.77.8.256	Asl4vm-app-san1 Asl4vm-app-san2	10.77.8.262 10.77.8.263	HTTP	8180 8080		no
http://ml-asl4.sisar.asl/	10.77.8.256	Asl4vm-app-san1	10.77.8.262	HTTP	8580		no
http://puacomuni-asl4.sardegna salute.it	10.77.8.256	Asl4vm-app-san1	10.77.8.262	HTTPS	8180		si
http://sian-asl4.sisar.asl/	10.77.8.256	Asl4vm-app-san1	10.77.8.262	HTTP	8089		no
http://smxint-areas-asl4.sisar.asl	10.77.8.256	Asl4vm-app-san1	10.77.8.262	HTTP	8080		no
http://soweb-asl4.sisar.asl/	10.77.8.256	Asl4vm-app-san1	10.77.8.262	HTTP	8280		no
http://spresal-asl4.sisar.asl/	10.77.8.256	Asl4vm-app-san2	10.77.8.263	HTTP	8380		no

Tabella 108 – Accessi esterni/interni ASL4

4.4.2.5.4.1 Flussi interni

4.4.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn	10.77.9.66 10.77.9.66	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA

	asl5vm-app-san2-psn								
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA

Tabella 109 – Flussi SIOAAP ASL4

4.4.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 110 – Flussi SIOAAP – Connessioni a DB

4.4.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL4	asl4-lbl1-psn asl4-lbl2-psn	10.77.8.230 10.77.8.231	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Application Server ASL4	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
----------------------------	--	----------------------------	------------	----------------------------------	--------------------------	------------	----	--	----------------

Tabella 111 – Flussi DNS ASL4

4.4.2.5.4.2 Flussi esterni

4.4.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Port a	Rea d \ wri te	Conten uto flusso
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	cot.aressardeg na.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integra zione con COT
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	interoperabilit a.inail.it	interoperabilita.ina il.it	93.147.161.1 49		TCP	443		PS Inail integra zione
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integra zione
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	cupweb.sisar.a sl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E- prescri ption integra zione
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integra zione
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	protocollo.sisa r.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protoc ollo Integra zione
areas-asl4.sisar.asl	asl4vm-app- san1-psn asl4vm-app- san2-psn	10.77.8.262 10.77.8.263	vip-picasso- cressan.sisar.a sl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integra zione Picasso (ADT- EDF)

Tabella 112 – Flussi SIOAAP ASL4

4.4.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 113 – Flussi SIOAAP – Connessioni a DB ASL4

4.4.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl4.sisar.asl	areas-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl4.sisar.asl	spresal-asl4.sisar.asl	10.77.8.256		TCP	80443		INTEGRAZIONE PICASSO

Tabella 114 – Flussi PICASSO ASL4

4.4.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

	04.cluster-okd.sisar.asl									
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 115 – Flussi PICASSO – Connessioni a DB ASL4

4.4.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl4vm-esb-san1				10.77.8.263			8080	R/W	tipo: http da spagic a WS; flusso: LIStoELIOT_RicezioneRichiesta
	asl4vm-app-san1-psn	10.77.8.262						6072	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl4vm-app-san2-psn	10.77.8.263						6072	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl4vm-esb-san1				10.77.8.263			8080	R/W	tipo: http da spagic a WS; flusso: PrintEtichettaEliot
	asl4vm-esb-san1				10.77.8.263			8080	R/W	tipo: http da spagic a WS; flusso: CambioStato
	asl4vm-esb-san1				10.77.8.263			8080	R/W	tipo: http da spagic a WS; flusso: CambioStatoDettaglio_ELIOT
	asl4vm-esb-san1				10.77.8.263			8080	R/W	tipo: http da spagic a WS; flusso: CambioStatoDettaglio

Sistema a source	Hostna me \ DNS source	IP source	Sistema destination	Hostnam e \ DNS destinati on	IP destination	Tipo sistem a estern o (SaaS, on prem ,...)	Protocol lo \ tecnolog ia	Port a	Rea d \ writ e	Contenuto flusso
	asl4vm- esb-san1				10.77.8.263			808 0	R/W	tipo: http da spagic a WS; flusso: Eliot_OE_Typescreen
	asl4vm- esb-san1				10.77.8.263			808 0	R/W	tipo: http da spagic a WS; flusso: ELIOT_TO_OE_SACCHE
	asl4vm- esb-san1				10.77.8.263			808 0	R/W	tipo: http da spagic a WS; flusso: OE_TrasfusionaleReperisciRisult atiHL7
	asl4vm- esb-san1				10.77.8.263			808 0	R/W	tipo: http da spagic a WS; flusso: TrasfSendRichiestaHL7
	asl4vm- esb-san1				10.77.8.263			808 0	R/W	tipo: http da spagic a WS; flusso: UpdDatiSangue

Tabella 116 – Flussi SPAGIC ASL4

4.4.2.5 Flussi e Accessibilità

4.4.2.6 Sicurezza

4.4.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.4.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegna.salute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.4.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E-prescription integr.
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263		10.96.62.139 10.96.62.140 10.96.62.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
asl4vm-app-san1-psn asl4vm-app-san2-psn	10.96.62.139 10.96.62.140 10.96.62.141		10.3.67.167 10.3.67.168 10.3.67.169		TCP	1521	Flussi Applicativi SIOAAP - db_link AMC (non presente in doc SardegnaIT)
asl4vm-app-san1-psn	10.77.8.262		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL4 to DNS CRESSAN
asl4vm-app-san2-psn	10.77.8.263		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL4 to DNS CRESSAN
asl4-lbl1-psn	10.77.8.230		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL4 to DNS CRESSAN
asl4-lbl2-psn	10.77.8.231		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL4 to DNS CRESSAN

Tabella 117 – Regole firewall ASL4

4.4.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.4.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl4vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl4vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl4-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl4-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 118 – Policy di backup ASL4

4.4.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.5 ASL 5 – ORISTANO

4.5.1 Architettura

L'architettura applicativa, rappresentata in Figura 6, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 6, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 5 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant ASL5, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl5.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'ASL5.

Nel layer di FrontEnd sono presenti due bilanciatori (asl5-lbl1-psn – asl5-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.5.1.1 Schema Logico

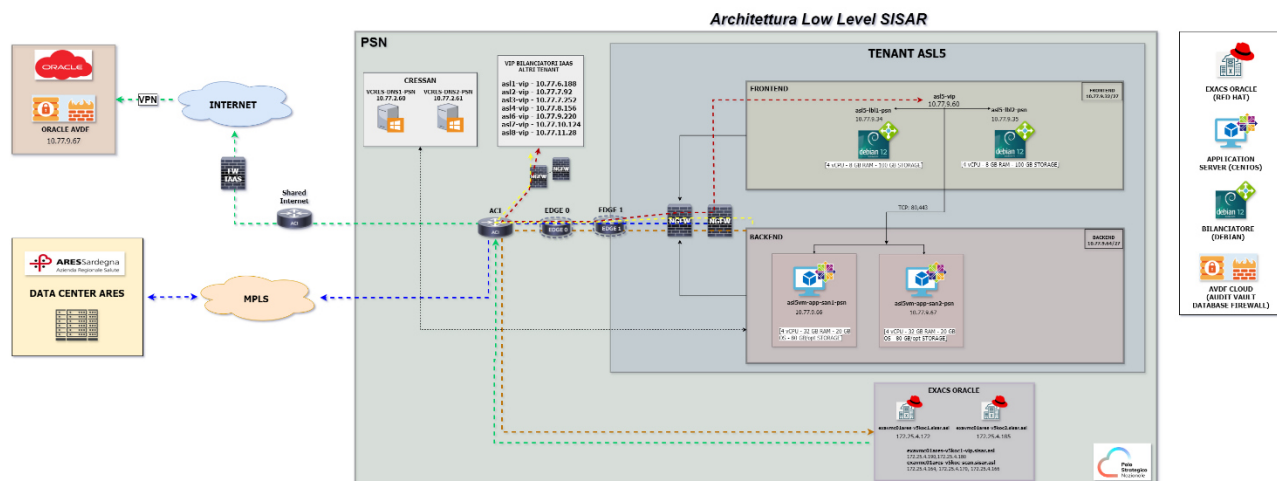


Figura 6 - Schema logico ASL5

4.5.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl5vm-app-san1-psn	ASL5	Application	Application Server	Virtuale	No
asl5vm-app-san2-psn	ASL5	Application	Application Server	Virtuale	No
asl5-vip-psn	ASL5	Presentation	Virtual IP	Virtuale	No
asl5-lbl1-psn	ASL5	Presentation	Balancer	Virtuale	No
asl5-lbl2-psn	ASL5	Presentation	Balancer	Virtuale	No
N/A	ASL5	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 119 – Lista componenti ASL5

4.5.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.5.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.5.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl5vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl5vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl5-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl5-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 120 – Caratteristiche ASL5

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.5.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl5vm-app-san1-psn	4	32	OS 20GB - /opt 80GB	SSD
asl5vm-app-san2-psn	4	32	OS 20GB - /opt 80GB	SSD
asl5-lbl1-psn	4	8	100	SSD
asl5-lbl2-psn	4	8	100	SSD

Tabella 121 – Dimensionamento ASL5

4.5.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl5vm-app-san1-psn	XFS	Non presente
asl5vm-app-san2-psn	XFS	Non presente
asl5-lbl1-psn	XFS	Non presente
asl5-lbl2-psn	XFS	Non presente

Tabella 122 – Composizione storage ASL5

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.5.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl5vm-app-san1-psn	10.77.9.66	PSN Industry Standard HA – Ambiente ASL05 - TGU servizio PSN02838349	10.77.9.64/27	N/A
asl5vm-app-san2-psn	10.77.9.67	PSN Industry Standard HA – Ambiente ASL05 - TGU servizio PSN02838349	10.77.9.64/27	N/A
asl5-vip	10.77.9.60	PSN Industry Standard HA – Ambiente ASL05 - TGU servizio PSN02838349	10.77.9.32/27	N/A
asl5-lbl1-psn	10.77.9.34	PSN Industry Standard HA – Ambiente ASL05 - TGU servizio PSN02838349	10.77.9.32/27	N/A
asl5-lbl2-psn	10.77.9.35	PSN Industry Standard HA – Ambiente ASL05 - TGU servizio PSN02838349	10.77.9.32/27	N/A

Tabella 123 – Piano di indirizzamento ASL5

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.5.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl5vm-app-san1-psn	<p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25 Tomcat version: 5.5.25 JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl5vm-app-san2-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl5-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl5-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 124 – Software installato ASL5

4.5.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl5vm-app-san1-psn	Tomcat	8	Open Source
asl5vm-app-san2-psn	Tomcat	8	Open Source

Tabella 125 – Web server ASL5

4.5.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL5PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 126 – Database server ASL5

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.5.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 127 - Server DNS ASL5

4.5.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 128 – Storage Condivisi ASL5

4.5.2.5 Networking

4.5.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.5.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	80	areas-asl5.sisar.asl	http://areas-asl5.sisar.asl/areas	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66:8080 10.77.9.66:8180 10.77.9.67:8080
asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	80	ml-asl5.sisar.asl	http://ml-asl5.sisar.asl/diagnosiFunzionaleAreas	asl5vm-app-san1-psn	10.77.9.66:8580
asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	80	sian-asl5.sisar.asl	http://sian-asl5.sisar.asl/SianWUI	asl5vm-app-san1-psn	10.77.9.66:8089
asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	80	spresal-asl5.sisar.asl	http://spresal-asl5.sisar.asl/Spresal	asl5vm-app-san1-psn	10.77.9.66:8380
asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	80	puacomuni-asl5.sardegna salute.it		asl5vm-app-san2-psn	10.77.9.67
asl5-lbl1-psn	10.77.9.34 10.77.9.35	80	soweb-asl5.sisar.asl		asl5vm-app-san2-psn	10.77.9.67:8280

asl5-lbl2-psn						
asl5-lbl1-psn	10.77.9.34	80		/LBLHealthCheck		localhost:5991
asl5-lbl2-psn	10.77.9.35					

Tabella 129 – Bilanciamento ASL5

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 130 – Tipo keepalive ASL5

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 131 – Tipo persistenza sessione ASL5

Tipologia balancing

Bilanciamento
Least Connection

Tabella 132 – Tipologia balancing ASL5

Tipo Domain Enable

Domain Enable
True

Tabella 133 – Tipo domain Enable ASL5

Type

Type
Adaptive

Tabella 134 – Type ASL5

4.5.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.9.34 10.77.9.35	10.77.9.60	asl5-lbl1-psn asl5-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl5.sardegna salute.it	Adaptive	true	pua-asl5.sisar.asl:80/pua pua-asl5.sisar.asl:80/ras-sp	redirect to LBL priv ASL5

Tabella 135 – Reverse proxy ASL5

4.5.2.5.4 Flussi e Accessibilità

4.5.2.5.4.1 Flussi interni

4.5.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn	10.77.9.66 10.77.9.67	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA

	asl5vm-app-san2-psn								
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA

Tabella 136 – Flussi SIOAAP ASL5

4.5.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas- asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 137 – Flussi SIOAAP – Connessioni a DB ASL5

4.5.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL5	asl5-lbl1-psn asl5-lbl2-psn	10.77.9.34 10.77.9.35	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server ASL5	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 138 – Flussi DNS ASL5

4.5.2.5.4.2 Flussi esterni

4.5.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas- asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	cot.aressardeгна.it	cot.aressardeгна.it	93.39.83.53		TCP	443		Integrazione con COT

areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	interoperabilita.ina il.it	interoperabilita.ina il.it	93.147.161.1 49		TCP	443		PS Inail integrazione
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E- prescription integrazione
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazione
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protocollo Integrazione
areas- asl5.sisar.asl	asl5vm-app- san1-psn asl5vm-app- san2-psn	10.77.9.66 10.77.9.67	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integrazione Picasso (ADT-EDF)

Tabella 139 – Flussi SIOAAP ASL5

4.5.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostna me \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo siste ma estern o (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Porta	Rea d \ writ e	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb- scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres- monitorps	vcres- monitor ps	10.3.67.2 33	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 140 – Flussi SIOAAP – Connessioni a DB ASL5

4.5.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl5.sisar.asl	areas-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl5.sisar.asl	spresal-asl5.sisar.asl	10.77.9.60		TCP	80443		INTEGRAZIONE PICASSO
---------------------	--------------------------------------	------------	------------------------	------------------------	------------	--	-----	-------	--	----------------------

Tabella 141 – Flussi PICASSO ASL5

4.5.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 142 – Flussi PICASSO – Connessioni a DB ASL5

4.5.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl5vm-app-san1-psn	10.77.9.66						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl5vm-app-san2-psn	10.77.9.66						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl5vm-esb-san1				10.77.9.67			8080	R/W	tipo: http da spagic a WS; flusso: InoltroToRad
	asl5vm-esb-san1				10.77.9.67			8080	R/W	tipo: http da spagic a WS; flusso: RadToOEChangeStatus
	asl5vm-esb-san1				10.77.9.67			8180	R/W	tipo: http da spagic a WS; flusso: ELIOT_TO_OE_SACCHE
	asl1vm-esb-san1	10.77.6.196						1521	R/W	Tutti i flussi

Tabella 143 – Flussi SPAGIC ASL5

4.5.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-asl5.sisar.asl/areas	10.77.9.60	Asl5vm-app-san1 Asl5vm-app-san2	10.77.9.66 10.77.9.67	HTTP	8080 8180		no
http://ml-asl5.sisar.asl/	10.77.9.60	Asl5vm-app-san1	10.77.9.66	HTTP	8580		no
http://sian-asl5.sisar.asl/	10.77.9.60	Asl5vm-app-san1	10.77.9.66	HTTP	8089		no
http://spresal-asl5.sisar.asl/	10.77.9.60	Asl5vm-app-san1	10.77.9.66	HTTP	8380		no
http://puacomuni-asl5.sardegna salute.it	10.77.9.60	Asl5vm-app-san2	10.77.9.67	HTTPS			si

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://soweb-asl5.sisar.asl/	10.77.9.60	Asl5vm-app-san2	10.77.9.67	HTTP	8280		no

Tabella 144 – Accessi esterni/interni ASL5

4.5.2.6 Sicurezza

4.5.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.5.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegna salute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.5.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail integrazione
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E- prescription integr.
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		10.128.102.139 10.128.102.140 10.128.102.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.128.102.139 10.128.102.140 10.128.102.141		10.3.67.167 10.3.67.168 10.3.67.169		TCP	1521	Flussi Applicativi SIOAAP - db_link AMC (non presente in doc SardegnaIT)
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.128.102.139 10.128.102.140 10.128.102.141		10.3.69.118 10.3.69.119 10.3.69.120		TCP	1521	Flussi Applicativi SIOAAP - db_link CUPWEB (non presente in doc SardegnaIT)
asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.67		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF) (non presente in doc SardegnaIT)
asl5vm-app-san1-psn	10.77.9.66		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL5 to DNS CRESSAN
asl5vm-app-san2-psn	10.77.9.67		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL5 to DNS CRESSAN
asl5-lbl1-psn	10.77.9.34		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL5 to DNS CRESSAN
asl5-lbl2-psn	10.77.9.35		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL5 to DNS CRESSAN

Tabella 145 – Regole firewall ASL5

4.5.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.5.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl5vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl5vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl5-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl5-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup ArchiveLog ogni 2 ore. 	30 gg

Tabella 146 – Policy di backup ASL5

4.5.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.6 ASL 6 – SANLURI

4.6.1 Architettura

L'architettura applicativa, rappresentata in Figura 7, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 7, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 6 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl6, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl6.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl6.

Nel layer di FrontEnd sono presenti due bilanciatori (asl6-lbl1-psn – asl6-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.6.1.1 Schema Logico

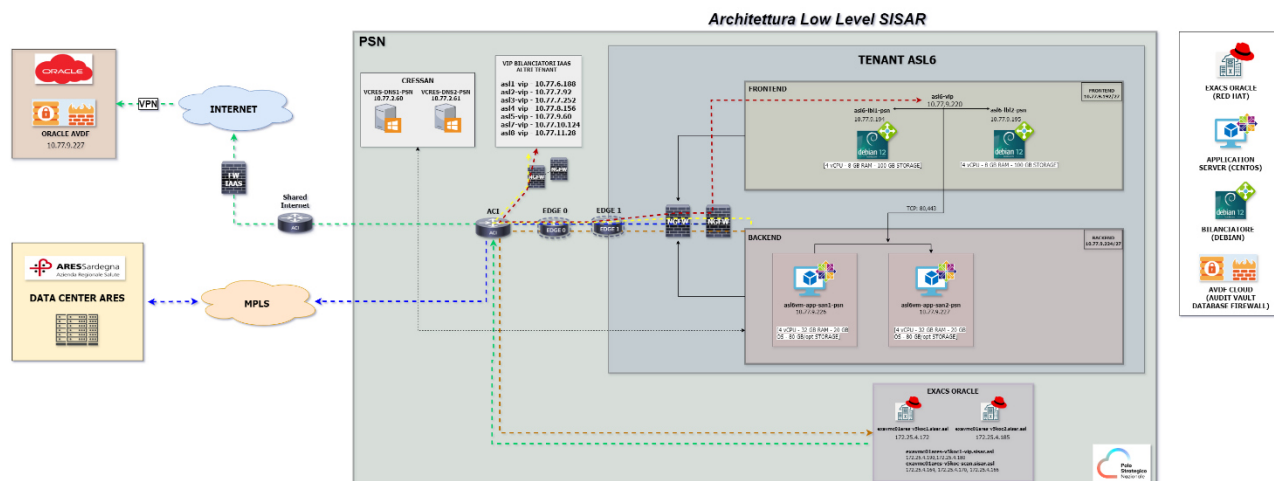


Figura 7 - Schema logico ASL6

4.6.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl6vm-app-san1-psn	ASL6	Application	Application Server	Virtuale	No
asl6vm-app-san2-psn	ASL6	Application	Application Server	Virtuale	No
asl6-vip-psn	ASL6	Presentation	Virtual IP	Virtuale	No
asl6-lbl1-psn	ASL6	Presentation	Balancer	Virtuale	No
asl6-lbl2-psn	ASL6	Presentation	Balancer	Virtuale	No
N/A	ASL6	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 147 – Lista componenti ASL6

4.6.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone)

costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.6.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.6.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl6vm-app-san1-psn	vSphere 8.0, VCDA \geq 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl6vm-app-san2-psn	vSphere 8.0, VCDA \geq 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl6-lbl1-psn	vSphere 8.0, VCDA \geq 10.3.x	VMWare	Debian	12 bookworm

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl6-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 148 – Caratteristiche ASL6

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.6.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl6vm-app-san1-psn	4	32	OS 20GB - /opt 80GB	SSD
asl6vm-app-san2-psn	4	32	OS 20GB - /opt 80GB	SSD
asl6-lbl1-psn	4	8	100	SSD
asl6-lbl2-psn	4	8	100	SSD

Tabella 149 – Dimensionamento ASL6

4.6.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl6vm-app-san1-psn	XFS	Non presente
asl6vm-app-san2-psn	XFS	Non presente
asl6-lbl1-psn	XFS	Non presente
asl6-lbl2-psn	XFS	Non presente

Tabella 150 – Composizione storage ASL6

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.6.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC
asl6vm-app-san1-psn	10.77.9.226	PSN Industry Standard HA – Ambiente ASL06 - TGU servizio PSN02838375	10.77.9.224/27	N/A
asl6vm-app-san1-psn	10.77.9.227	PSN Industry Standard HA – Ambiente ASL06 - TGU servizio PSN02838375	10.77.9.224/27	N/A
asl6-vip	10.77.9.220	PSN Industry Standard HA – Ambiente ASL06 - TGU servizio PSN02838375	10.77.9.192/27	N/A
asl6-lbl1-psn	10.77.9.194	PSN Industry Standard HA – Ambiente ASL06 - TGU servizio PSN02838375	10.77.9.192/27	N/A
asl6-lbl2-psn	10.77.9.195	PSN Industry Standard HA – Ambiente ASL06 - TGU servizio PSN02838375	10.77.9.192/27	N/A

Tabella 151 – Piano di indirizzamento ASL6

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.6.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl6vm-app-san1-psn	<p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: Unknown JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl6vm-app-san2-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl6-lbl1-psn	Oplon Secure Access v10	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl6-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 152 – Software installato ASL6

4.6.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl6vm-app-san1-psn	Tomcat	8	Open Source
asl6vm-app-san2-psn	Tomcat	8	Open Source

Tabella 153 – Web server ASL6

4.6.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL6PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 154 – Database server ASL6

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.6.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 155 - Server DNS ASL6

4.6.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r,...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 156 – Storage condivisi ASL6

4.6.2.5 Networking

4.6.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.6.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	areas-asl6.sisar.asl	http://areas-asl6.sisar.asl/areas	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226:8080 10.77.9.226:8180 10.77.9.227:8080
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	ml-asl6.sisar.asl	http://ml-asl6.sisar.asl/diagnosiFunzionaleAreas	asl6vm-app-san1-psn	10.77.9.226:8580
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	spresal-asl6.sisar.asl	http://spresal-asl6.sisar.asl/Spresal	asl6vm-app-san1-psn	10.77.9.226:8380
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	puacomuni- asl6.sardegna salute.it		asl6vm-app-san2-psn	10.77.9.227:8180
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	soweb-asl6.sisar.asl		asl6vm-app-san2-psn	10.77.9.227:8280
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	sian-asl6.sisar.asl	http://sian-asl6.sisar.asl/SianWUI	asl6vm-app-san1-psn	10.77.9.226:8089
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80	smxint-areas- asl6.sisar.asl	http://smxint-areas-asl6.sisar.asl/demone/		
asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	80		/LBLHealthCheck		localhost:5991

Tabella 157 – Bilanciamento ASL6

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 158 – Tipo keepalive ASL6

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 159 – Tipo persistenza sessione ASL6

Tipologia balancing

Bilanciamento
Least Connection

Tabella 160 – Tipologia balancing ASL6

Tipo Domain Enable

Domain Enable
True

Tabella 161 – Tipo domain enable ASL6

Type

Type
Adaptive

Tabella 162 – Type- ASL6

4.6.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.9.194 10.77.9.195	10.77.9.220	asl6-lbl1-psn asl6-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl6.sardegna salute.it	Adaptive	true	pua- asl6.sisar.asl:80/pua	redirect to LBL priv ASL6
								pua- asl6.sisar.asl:80/ras- sp	

Tabella 163 – Reverse proxy ASL6

4.6.2.5.4 Flussi e Accessibilità

4.6.2.5.4.1 Flussi interni

4.6.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn	10.77.8.2 10.77.8.3	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA

	asl3vm-app-san2-psn								
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA

Tabella 164 – Flussi SIOAAP ASL6

4.6.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 165 – Flussi SIOAAP – Connessioni a DB ASL6

4.6.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL6	asl6-lbl1-psn asl6-lbl2-psn	10.77.9.194 10.77.9.195	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server ASL6	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 166 – Flussi DNS ASL6

4.6.2.5.4.2 Flussi esterni

4.6.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integrazione con COT
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	interoperabilita.ina il.it	interoperabilita.ina il.it	93.147.161.149		TCP	443		PS Inail integrazione
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E-prescription integrazione

areas- asl6.sisar.asl	asl6vm-app- san1-psn asl6vm-app- san2-psn	10.77.9.226 10.77.9.227	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integraz ione
areas- asl6.sisar.asl	asl6vm-app- san1-psn asl6vm-app- san2-psn	10.77.9.226 10.77.9.227	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protoc ollo Integraz ione
areas- asl6.sisar.asl	asl6vm-app- san1-psn asl6vm-app- san2-psn	10.77.9.226 10.77.9.227	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integraz ione Picasso (ADT- EDF)

Tabella 167 – Flussi SIOAAP ASL6

4.6.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostna me \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo siste ma estern o (SaaS, on prem ,...)	Protocol lo \ tecnol ogia	Port a	Rea d \ writ e	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	152 1		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb- scan.sisar.asl	Listener EXACS		TCP	152 1		db_link CUPWEB
vcres- monitorps	vcres- monitor ps	10.3.67.2 33	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		talend - monitor PS

Tabella 168 – Flussi SIOAAP – Connessioni a DB ASL6

4.6.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Port a	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node- 01.cluster- okd.sisar.asl	10.3.61.50	areas- asl6.sisar.asl	areas- asl6.sisar.asl	10.77.9.220		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 02.cluster- okd.sisar.asl	10.3.61.51	areas- asl6.sisar.asl	areas- asl6.sisar.asl	10.77.9.220		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 03.cluster- okd.sisar.asl	10.3.61.52	areas- asl6.sisar.asl	areas- asl6.sisar.asl	10.77.9.220		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node- 04.cluster- okd.sisar.asl	10.3.61.53	areas- asl6.sisar.asl	areas- asl6.sisar.asl	10.77.9.220		TCP	80 443		INTEGRAZI ONE PICASSO

Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl6.sisar.asl	areas-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl6.sisar.asl	areas-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl6.sisar.asl	areas-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl6.sisar.asl	areas-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl6.sisar.asl	areas-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl6.sisar.asl	spresal-asl6.sisar.asl	10.77.9.220		TCP	80443		INTEGRAZIONE PICASSO

Tabella 169 – Flussi PICASSO

4.6.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ Write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

	- okd.sisar. asl									
Worker Node Picasso	worker- node- 02.cluster - okd.sisar. asl	10.3.61. 51	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 03.cluster - okd.sisar. asl	10.3.61. 52	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 04.cluster - okd.sisar. asl	10.3.61. 53	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 05.cluster - okd.sisar. asl	10.3.61. 54	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 06.cluster - okd.sisar. asl	10.3.61. 55	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 07.cluster - okd.sisar. asl	10.3.61. 56	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 08.cluster - okd.sisar. asl	10.3.61. 57	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 09.cluster - okd.sisar. asl	10.3.61. 58	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO

Tabella 170 – Flussi PICASSO – Connessioni a DB ASL6

4.6.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas- asl6.sisar.asl/areas	10.77.9.220	Asl6vm-app- san1 Asl6vm-app- san2	10.77.9.226 10.77.9.227	HTTP	8080 8180		no
http://ml-asl6.sisar.asl/	10.77.9.220	Asl6vm-app- san1	10.77.9.226	HTTP	8580		no
http://spresal-asl6.sisar.asl/	10.77.9.220	Asl6vm-app- san1	10.77.9.226	HTTP	8380		no
http://puacomuni- asl6.sardegna salute.it	10.77.9.220	Asl6vm-app- san2	10.77.9.227	HTTPS	8180		si
http://soweb-asl6.sisar.asl/	10.77.9.220	Asl6vm-app- san2	10.77.9.227	HTTP	8280		no
http://eliot.aslnuoro.it	10.77.9.220	Asl6vm-app- san1 Asl6vm-app- san2	10.77.9.226 10.77.9.227	HTTP			no

Tabella 171 – Accessi esterni/interni ASL6

4.6.2.6 Sicurezza

4.6.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.6.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegna salute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.6.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP -MD. LEG. vs INPS
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E- prescription integr.
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		10.240.62.139 10.240.62.140 10.240.62.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
asl6vm-app-san1- psn asl6vm-app-san2- psn	10.77.9.226 10.77.9.227		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT- EDF) (non presente in doc SardegnaIT)
asl6vm-app-san1- psn	10.77.9.226		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL6 to DNS CRESSAN
asl6vm-app-san2- psn	10.77.9.227		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL6 to DNS CRESSAN
asl6-lbl1-psn	10.77.9.194		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL6 to DNS CRESSAN
asl6-lbl2-psn	10.77.9.195		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL6 to DNS CRESSAN

Tabella 172 – Regole firewall ASL6

4.6.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.6.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl6vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl6vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl6-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl6-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup ArchiveLog ogni 2 ore. 	30 gg

Tabella 173 – Policy di backup ASL6

4.6.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.7 ASL 7 – CARBONIA

4.7.1 Architettura

L'architettura applicativa, rappresentata in Figura 8, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 8, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 7 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl7, per mezzo della VRF.

Il traffico internet proveniente dal portale ***puacomuni-asl7.sardegna salute.it*** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl7.

Nel layer di FrontEnd sono presenti due bilanciatori (asl7-lbl1-psn – asl7-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.7.1.1 Schema Logico

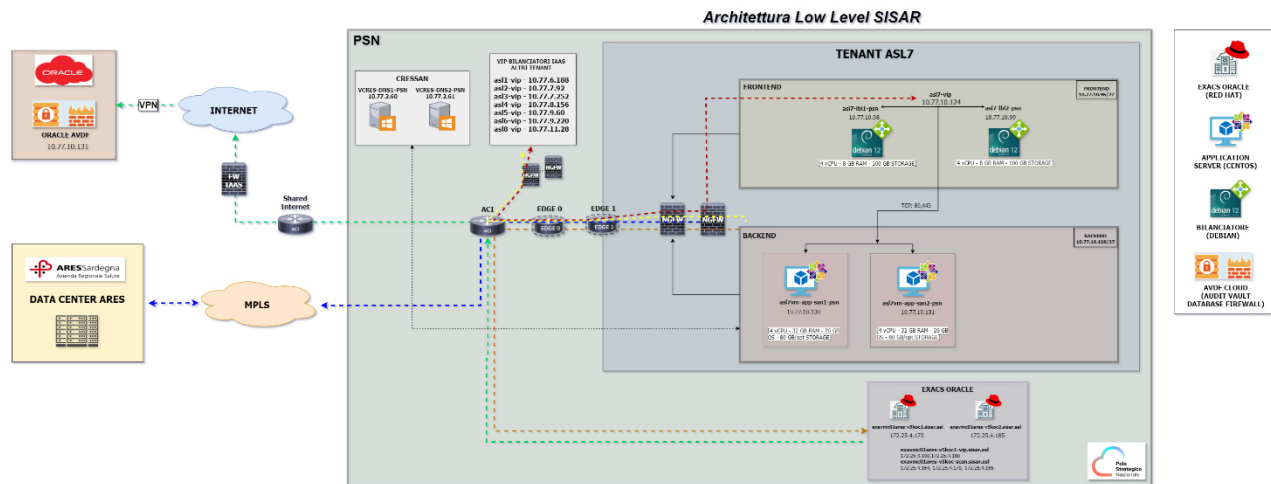


Figura 8 - Schema logico ASL7

4.7.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl7vm-app-san1-psn	ASL7	Application	Application Server	Virtuale	No
asl7vm-app-san2-psn	ASL7	Application	Application Server	Virtuale	No
asl7-vip-psn	ASL7	Presentation	Virtual IP	Virtuale	No
asl7-lbl1-psn	ASL7	Presentation	Balancer	Virtuale	No
asl7-lbl2-psn	ASL7	Presentation	Balancer	Virtuale	No
N/A	ASL7	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 174 – Lista componenti ASL7

4.7.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.7.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.7.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl7vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl7vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl7-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl7-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 175 – Caratteristiche ASL7

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.7.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl7vm-app-san1-psn	4	32	OS 20GB - /opt 80GB	SSD
asl7vm-app-san2-psn	4	32	OS 20GB - /opt 80GB	SSD
asl7-lbl1-psn	4	8	100	SSD
asl7-lbl2-psn	4	8	100	SSD

Tabella 176 – Dimensionamento ASL7

4.7.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl7vm-app-san1-psn	XFS	Non presente
asl7vm-app-san2-psn	XFS	Non presente
asl7-lbl1-psn	XFS	Non presente
asl7-lbl2-psn	XFS	Non presente

Tabella 177 – Composizione Storage ASL7

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.7.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl7vm-app-san1-psn	10.77.10.130	PSN Industry Standard HA – Ambiente ASL07 - TGU servizio PSN02838457	10.77.10.128/27	N/A
asl7vm-app-san2-psn	10.77.10.131	PSN Industry Standard HA – Ambiente ASL07 - TGU servizio PSN02838457	10.77.10.128/27	N/A
asl7-vip	10.77.10.124	PSN Industry Standard HA – Ambiente ASL07 - TGU servizio PSN02838457	10.77.10.96/27	N/A
asl7-lbl1-psn	10.77.10.98	PSN Industry Standard HA – Ambiente ASL07 - TGU servizio PSN02838457	10.77.10.96/27	N/A
asl7-lbl2-psn	10.77.10.99	PSN Industry Standard HA – Ambiente ASL07 - TGU servizio PSN02838457	10.77.10.96/27	N/A

Tabella 178 – Piano di indirizzamento ASL7

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.7.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl7vm-app-san1-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl7vm-app-san2-psn	<p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_10</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl7-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl7-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 179 – Software installato ASL7

4.7.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl7vm-app-san1-psn	Tomcat	8	Open Source
asl7vm-app-san2-psn	Tomcat	8	Open Source

Tabella 180 – Web server ASL7

4.7.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	ASL7PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 181 – Database server ASL7

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.7.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 182 - Server DNS ASL7

4.7.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 183 – Storage Condivisi ASL7

4.7.2.5 Networking

4.7.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.7.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	areas-asl7.sisar.asl	http://areas-asl7.sisar.asl/areas	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130:8080 10.77.10.130:8180 10.77.10.131:8080
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	soweb-asl7.sisar.asl	http://soweb-asl7.sisar.asl/	asl7vm-app-san1-psn	10.77.10.130:8280
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	ml-asl7.sisar.asl	http://ml-asl7.sisar.asl/diagnosiFunzionaleAreas	asl7vm-app-san1-psn	10.77.10.130:8580
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	sian-asl7.sisar.asl	http://sian-asl7.sisar.asl/SianWUI/SianWUI/SianWS	asl7vm-app-san1-psn	10.77.10.130:8089
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	spresal-asl7.sisar.asl	http://spresal-asl7.sisar.asl/Spresal	asl7vm-app-san2-psn	10.77.10.131:8380
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	puacomuni-asl7.sardegnaalute.it	/pua/ras-sp	asl7vm-app-san2-psn	10.77.10.131:8080
asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	80	Healthcheck	/LBLHealthCheck	asl7vm-app-san2-psn	localhost:5991

Tabella 184 – Bilanciamento ASL7

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 185 – Tipo keepalive ASL7

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 186 – Tipo persistenza sessione ASL7

Tipologia balancing

Bilanciamento
Least Connection

Tabella 187 – Tipologia balancing ASL7

Tipo Domain Enable

Domain Enable
True

Tabella 188 – Tipo domain enable ASL7

Type

Type
Adaptive

Tabella 189 – Type ASL7

4.7.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.10.98 10.77.10.99	10.77.10.124	asl7-lbl1-psn asl7-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl7.sardegna salute.it	Adaptive	true	<p>puaslar.sisar.asl:80/pua</p> <p>puaslar.sisar.asl:80/ras-sp</p>	<p>redirect to LBL priv ASL7</p>

Tabella 190 – Reverse proxy ASL7

4.7.2.5.4 Flussi e Accessibilità

4.7.2.5.4.1 Flussi interni

4.7.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn	10.77.8.2 10.77.8.3	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA

	asl3vm-app-san2-psn								
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA

Tabella 191 – Flussi SIOAAP ASL7

4.7.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 192 – Flussi SIOAAP – Connessioni a DB ASL7

4.7.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL7	asl7-lbl1-psn asl7-lbl2-psn	10.77.10.98 10.77.10.99	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Application Server ASL7	asl7vm-app- san1-psn asl7vm-app- san2-psn	10.77.10.130 10.77.10.131	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
----------------------------	--	------------------------------	------------	----------------------------------	--------------------------	------------	----	--	----------------

Tabella 193 – Flussi DNS ASL7

4.7.2.5.4.2 Flussi esterni

4.7.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo siste ma estern o (SaaS, on prem ,...)	Prot ocol lo \ tec nol ogia	Port a	Rea d \ writ e	Conten uto flusso
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integraz ione con COT
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	interoperabilita.ina il.it	interoperabilita.ina il.it	93.147.161.14 9		TCP	443		PS Inail integrazi one
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integraz ione
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E- prescrip tion integrazi one
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazi one

areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protocol lo Integraz ione
areas- asl7.sisar.asl	asl7vm- app-san1- psn asl7vm- app-san2- psn	10.77.10.130 10.77.10.131	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integraz ione Picasso (ADT- EDF)

Tabella 194 – Flussi SIOAAP ASL7

4.7.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostna me \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 195 – Flussi SIOAAP – Connessioni a DB ASL7

4.7.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas- asl7.sisar.asl	areas- asl7.sisar.asl	10.77.10.124		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas- asl7.sisar.asl	areas- asl7.sisar.asl	10.77.10.124		TCP	80 443		INTEGRAZI ONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas- asl7.sisar.asl	areas- asl7.sisar.asl	10.77.10.124		TCP	80 443		INTEGRAZI ONE PICASSO

Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl7.sisar.asl	areas-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl7.sisar.asl	spresal-asl7.sisar.asl	10.77.10.124		TCP	80443		INTEGRAZIONE PICASSO

Tabella 196 – Flussi PICASSO ASL7

4.7.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 197 – Flussi PICASSO – Connessioni a DB ASL7

4.7.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-asl7.sisar.asl/areas	10.77.10.124	Asl7vm-app-san1 Asl7vm-app-san2	10.77.10.130 10.77.10.131	HTTP	8080 8180		no
http://soweb-asl7.sisar.asl/	10.77.10.124	Asl7vm-app-san1	10.77.10.130	HTTP	8280		no
http://ml-asl7.sisar.asl/	10.77.10.124	Asl7vm-app-san1	10.77.10.130	HTTP	8580		no
http://sian-asl7.sisar.asl/	10.77.10.124	Asl7vm-app-san1	10.77.10.130	HTTP	8089		no
http://spresal-asl7.sisar.asl/	10.77.10.124	Asl7vm-app-san2	10.77.10.131	HTTP	8380		no
http://puacomuni-asl7.sardegna salute.it	10.77.10.124	Asl7vm-app-san2	10.77.10.131	HTTPS	8080		si

Tabella 198 – Accessi esterni/interni ASL7

4.7.2.6 Sicurezza

4.7.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.7.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegna salute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.7.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E-prescription integr.
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		10.80.62.139 10.80.62.140 10.80.62.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF) (non presente in doc SardegnaIT)
asl7vm-app-san1-psn	10.77.10.130		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL7 to DNS CRESSAN
asl7vm-app-san2-psn	10.77.10.131		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL7 to DNS CRESSAN
asl7-lbl1-psn	10.77.10.98		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL7 to DNS CRESSAN
asl7-lbl2-psn	10.77.10.99		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL7 to DNS CRESSAN

Tabella 199 – Regole firewall ASL7

4.7.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.7.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl7vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl7vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl7-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl7-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 200 – Policy di backup ASL7

4.7.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.8 ASL 8 – CAGLIARI

4.8.1 Architettura

L'architettura applicativa, rappresentata in Figura 9, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud. La stessa implementazione del servizio di database Oracle menzionato sarà utilizzata sia dal tenant ALS 8 di Cagliari che dal tenant AOUCA, in continuità con l'architettura attualmente in esercizio on-premise. Non è possibile dedicare un DBMS Oracle ad uso esclusivo del tenant AOUCA a causa delle seguenti problematiche:

- È necessario stimare e realizzare un intervento per estendere l'interoperabilità anagrafica e adeguare le integrazioni dei sistemi dipartimentali coinvolti con sistemi esterni.
- Si verificherebbe una perdita di univocità dell'ID Paziente dipartimentale nei confronti di sistemi di terze parti, con conseguenti gravi disservizi e rischi di anomalie sui dati.
- I sistemi di terze parti non sono predisposti a ricevere richieste o inviare aggiornamenti di stato a endpoint diversi.
- Le attuali interazioni tramite DBLink richiederebbero una reingegnerizzazione delle integrazioni.
- Non sarebbe possibile effettuare la migrazione di sicurezza inversa con Golden Gate, precludendo un piano di rollback in caso di esito migratorio non conforme alle previsioni.
- La pianificazione della migrazione subirebbe ritardi.

Pertanto, ASL 8 di Cagliari e AOUCA condivideranno la stessa infrastruttura DBMS Oracle su Exadata, pur disponendo di infrastrutture IaaS Shared HA dedicate.

L'architettura di sicurezza, rappresentata in Figura 9, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ASL 8 è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Asl8, per mezzo della VRF.

Il traffico internet proveniente dal portale **puacomuni-asl8.sardegna salute.it** viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl8.

Nel layer di FrontEnd sono presenti due bilanciatori (asl8-lbl1-psn – asl8-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.8.1.1 Schema Logico

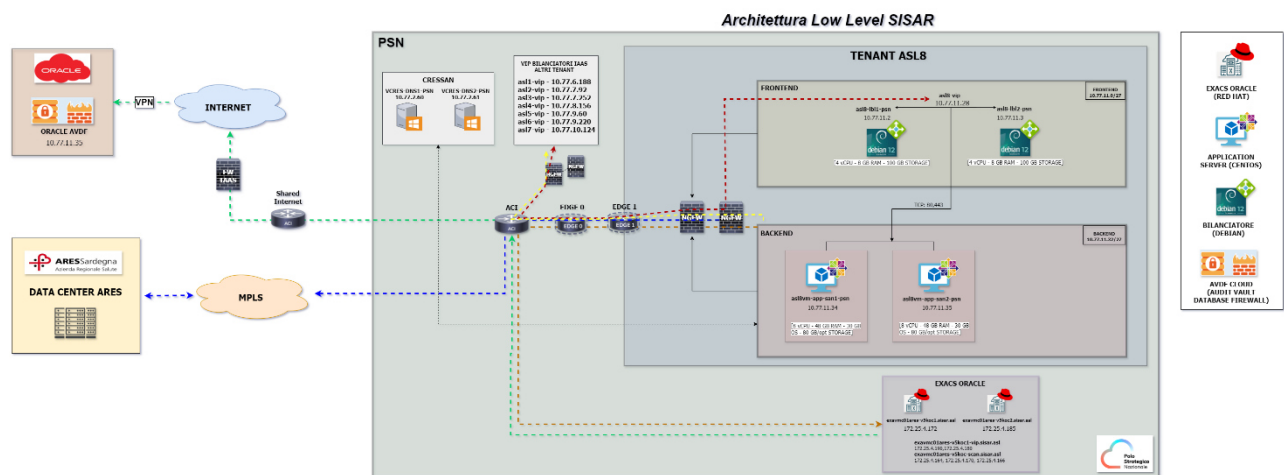


Figura 9 - Schema logico ASL8

4.8.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
asl8vm-app-san1-psn	ASL8	Application	Application Server	Virtuale	No
asl8vm-app-san2-psn	ASL8	Application	Application Server	Virtuale	No
asl8-vip-psn	ASL8	Presentation	Virtual IP	Virtuale	No
asl8-lbl1-psn	ASL8	Presentation	Balancer	Virtuale	No
asl8-lbl2-psn	ASL8	Presentation	Balancer	Virtuale	No
N/A	ASL8	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 201 – Lista componenti ASL8

4.8.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.8.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.8.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
asl8vm-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl8vm-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
asl8-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
asl8-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 202 – Caratteristiche ASL8

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.8.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
asl8vm-app-san1-psn	8	48	OS 30GB - /opt 80GB	SSD
asl8vm-app-san2-psn	8	48	OS 30GB - /opt 80GB	SSD
asl8-lbl1-psn	4	8	100	SSD
asl8-lbl2-psn	4	8	100	SSD

Tabella 203 – Dimensionamento ASL8

4.8.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
asl8vm-app-san1-psn	XFS	Non presente
asl8vm-app-san2-psn	XFS	Non presente
asl8-lbl1-psn	XFS	Non presente
asl8-lbl2-psn	XFS	Non presente

Tabella 204 – Composizione storage ASL8

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.8.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
asl8vm-app-san1-psn	10.77.11.34	PSN Industry Standard HA – Ambiente ASL08 - TGU servizio PSN02838493	10.77.11.32/27	N/A
asl8vm-app-san2-psn	10.77.11.35	PSN Industry Standard HA – Ambiente ASL08 - TGU servizio PSN02838493	10.77.11.32/27	N/A
asl8-vip	10.77.11.38	PSN Industry Standard HA – Ambiente ASL08 - TGU servizio PSN02838493	10.77.11.0/27	N/A
asl8-lbl1-psn	10.77.11.2	PSN Industry Standard HA – Ambiente ASL08 - TGU servizio PSN02838493	10.77.11.0/27	N/A
asl8-lbl2-psn	10.77.11.3	PSN Industry Standard HA – Ambiente ASL08 - TGU servizio PSN02838493	10.77.11.0/27	N/A

Tabella 205 – Piano di indirizzamento ASL8

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.8.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl8vm-app-san1-psn	Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181 -----	Servizi Applicativi	NO	ASK DEV	Open Source
	Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_aouca Tomcat version: 8.0.35 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181				

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
asl8vm-app-san2-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_asl8 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_24</p>	Servizi Applicativi	NO	ASK DEV	Open Source
asl8-lbl1-psn	Oplon OSA 10.10.003	Load Balancer - Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)
asl8-lbl2-psn	Oplon OSA 10.10.003	Load Balancer - Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 206 – Software installato ASL8

4.8.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
asl8vm-app-san1-psn	Tomcat	8	Open Source
asl8vm-app-san2-psn	Tomcat	8	Open Source

Tabella 207 – Web Server ASL8

4.8.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares- v5koc1.sisar.asl exavmc01ares- v5koc2.sisar.asl	ASL8PDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 208 – Database server ASL8

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.8.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 209 - Server DNS ASL8

4.8.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r,...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 210 – Storage condivisi ASL8

4.8.2.5 Networking

4.8.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.8.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciato re	Porte Bilanciato re	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	puacomuni- asl8.sardegna salute.it		aouca-app-san1-psn	10.77.11.34:83 80
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	areas-asl8.sisar.asl	http://areas-asl8.sisar.asl/areas	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34:84 80 10.77.11.35:84 80 10.77.11.35:83 80
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	sian-asl8.sisar.asl	http://sian-asl8.sisar.asl/SianWUI	aouca-app-san1-psn	10.77.11.34:80 89
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	soweb- asl8.sisar.asl		aouca-app-san2-psn	10.77.11.35:82 82
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	://spresal- asl8.sisar.asl	http://spresal-asl8.sisar.asl/Spresal	aouca-app-san2-psn	10.77.11.35:86 80
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80	ml-asl8.sisar.asl	http://ml- asl8.sisar.asl/diagnosiFunzionaleAreas	aouca-app-san2-psn	10.77.11.35:85 80
asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	80		/LBLHealthCheck		localhost:5991

Tabella 211 – Bilanciamento ASL8

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 212 – Tipo keepalive ASL8

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 213 – Tipo persistenza sessione ASL8

Tipologia balancing

Bilanciamento
Least Connection

Tabella 214 – Tipologia balancing ASL8

Tipo Domain Enable

Domain Enable
True

Tabella 215 – Tipo domain enable ASL8

Type

Type
Adaptive

Tabella 216 – Type ASL8

4.8.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.11.2	10.77.11.38	asl8-lbl1-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl8.sardegna salute.it	Adaptive	true	pu-comuni-asl8.sardegna salute.it:80/pua	redirect to LBL priv ASL8
10.77.11.3		asl8-lbl2-psn						pu-comuni-asl8.sardegna salute.it:80/ras-sp	

Tabella 217 – Reverse proxy ASL8

4.8.2.5.4 Flussi e Accessibilità

4.8.2.5.4.1 Flussi interni

4.8.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn	10.77.8.2 10.77.8.3	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA

	asl3vm-app-san2-psn								
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA

Tabella 218 – Flussi SIOAAP ASL8

4.8.2.5.4.1.2 Flussi SIOAAP - Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 219 – Flussi SIOAAP – Connessioni a DB ASL8

4.8.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ASL8	asl8-lbl1-psn asl8-lbl2-psn	10.77.11.2 10.77.11.3	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Application Server ASL8	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
----------------------------	--	----------------------------	------------	----------------------------------	--------------------------	------------	----	--	----------------

Tabella 220 – Flussi DNS ASL8

4.8.2.5.4.2 Flussi esterni

4.8.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo siste ma estern o (SaaS, on prem ,...)	Proto collo \ tecnol ogia	Port a	R e a d \ w r i t e	Conten uto flusso
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integraz ione con COT
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	interoperabilita.ina il.it	interoperabilita.ina il.it	93.147.161.14 9		TCP	443		PS Inail integrazi one
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integraz ione
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E- prescrip tion integrazi one
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazi one
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protoco llo Integraz ione
areas- asl8.sisar.asl	aouca-app- san1-psn aouca-app- san2-psn	10.77.11.34 10.77.11.35	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integraz ione Picasso (ADT- EDF)

Tabella 221 – Flussi SIOAAP

4.8.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 222 – Flussi SIOAAP – Connessioni a DB ASL8

4.8.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-asl8.sisar.asl	areas-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	spresal-asl8.sisar.asl	spresal-asl8.sisar.asl	10.77.11.38		TCP	80443		INTEGRAZIONE PICASSO

Tabella 223 – Flussi PICASSO ASL8

4.8.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 224 – Flussi PICASSO Connessione a DB - ASL8

4.8.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	asl8vm-app-san1-psn	10.77.11.34						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl8vm-app-san2-psn	10.77.11.35						5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	asl8vm-esb-san2				10.77.13.5			6082	R/W	servizio http da spagic asl8 a spagic aob; flusso: PrintEtichettaEliot_Eliot

Tabella 225 – Flussi SPAGIC ASL8

4.8.2.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://puacomuni-asl8.sardegناسalute.it	10.77.11.38	Aouca-app-san1	10.77.11.34	HTTPS	8380		si
http://areas-asl8.sisar.asl/areas	10.77.11.38	Aouca-app-san1 Aouca-app-san2	10.77.11.34 10.77.11.35	HTTP	8380 8480		no
http://sian-asl8.sisar.asl/	10.77.11.38	Aouca-app-san1	10.77.11.34	HTTP	8089		no
http://soweb-asl8.sisar.asl/	10.77.11.38	Aouca-app-san2	10.77.11.35	HTTP	8282		no
http://spresal-asl8.sisar.asl/	10.77.11.38	Aouca-app-san2	10.77.11.35	HTTP	8680		no
http://ml-asl8.sisar.asl/	10.77.11.38	Aouca-app-san2	10.77.11.35	HTTP	8580		no

Tabella 226 – Accessi esterni/interni ASL8

4.8.2.6 Sicurezza

4.8.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale. Il servizio PUA Comuni è stato integrato con Access Manager regionale della RAS utilizzando il protocollo SAML2. Per comprendere meglio il comportamento dell'Access Manager durante tutto il processo di autenticazione, vengono descritti in *Figura 2 - Autenticazione Pua Comuni* i passi seguiti durante l'accesso di un utente al servizio PUA Comuni mediante browser web utilizzando di protocollo SAML.

4.8.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegناسalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.8.2.6.3 Regole Firewall

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP - MD. LEG. vs INPS
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E-prescription integr.
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl1-vip	10.77.6.188	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl2-vip	10.77.7.92	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl3-vip	10.77.7.252	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA

Hostname Sorgente	Rete / IP Sorgente	Hostname Destinazione	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl4-vip	10.77.8.256	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl5-vip	10.77.9.60	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl6-vip	10.77.9.220	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl7-vip	10.77.10.124	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35	asl8-vip	10.77.11.38	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		10.66.2.139 10.66.2.140 10.66.2.141		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
asl8vm-app-san1-psn asl8vm-app-san2-psn	10.77.11.34 10.77.11.35		10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF) (non presente in doc SardegnaIT)
asl8vm-app-san1-psn	10.77.11.34		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL8 to DNS CRESSAN
asl8vm-app-san2-psn	10.77.11.35		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL8 to DNS CRESSAN
asl8-lbl1-psn	10.77.11.2		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL8 to DNS CRESSAN
asl8-lbl2-psn	10.77.11.3		10.77.2.60 10.77.2.61		TCP/UDP	53	from ASL8 to DNS CRESSAN

Tabella 227 – Regole firewall ASL8

4.8.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.8.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
aouca-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouca-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl8-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl8-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 228 – Policy di backup ASL8

4.8.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.9 ARNAS

4.9.1 Architettura

L'architettura applicativa, rappresentata in Figura 10, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 10, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSSAN e tenant ARNAS è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant Arnas, per mezzo della VRF.

Il traffico Internet viene redirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant Arnas.

Nel layer di FrontEnd sono presenti due bilanciatori (brotzu-lbl1-psn – brotzu-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.9.1.1 Schema Logico

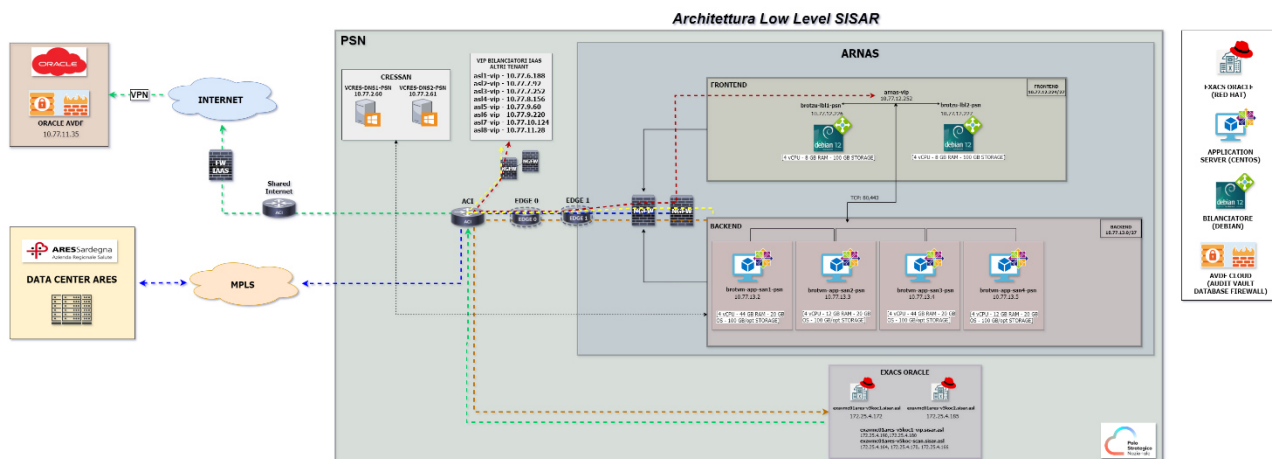


Figura 10 - Schema logico ARNAS

4.9.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
brotmvm-app-san1-psn	ARNAS	Application	Application Server	Virtuale	No
brotmvm-app-san2-psn	ARNAS	Application	Application Server	Virtuale	No
brotmvm-app-san3-psn	ARNAS	Application	Application Server	Virtuale	No
brotmvm-app-san4-psn	ARNAS	Application	Application Server	Virtuale	No
arnas-vip-psn	ARNAS	Presentation	Balancer	Virtuale	No
brotmvm-lbl1-psn	ARNAS	Presentation	Balancer	Virtuale	No
brotmvm-lbl2-psn	ARNAS	Presentation	Balancer	Virtuale	No
N/A	ARNAS	Data	Oracle Exadata Cloud at Service	Virtuale	No
N/A	Oracle Cloud	Data	ORACLE AVDF CLOUD	Virtuale	No

Tabella 229 – Lista Componenti ARNAS

4.9.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

4.9.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.9.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
brotvm-app-san1-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
brotvm-app-san2-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
brotvm-app-san3-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
brotvm-app-san4-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
brotzu-lbl1-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	Debian	12 bookworm
brotzu-lbl2-psn	vSphere 8.0, VCDa ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 230 – Caratteristiche ARNAS

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.9.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
brotvm-app-san1-psn	4	44	OS 20GB - /opt 100GB	SSD
brotvm-app-san2-psn	4	12	OS 20GB - /opt 100GB	SSD
brotvm-app-san3-psnc	4	44	OS 20GB - /opt 100GB	SSD
brotvm-app-san4-psnc	4	12	OS 20GB - /opt 100GB	SSD
brotzu-lbl1-psn	4	8	100	SSD
brotzu-lbl2-psn	4	8	100	SSD

Tabella 231 – Dimensionamento ARNAS

4.9.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
brotvm-app-san1-psn	XFS	Non presente
brotvm-app-san2-psn	XFS	Non presente
brotvm-app-san3-psnc	XFS	Non presente
brotvm-app-san4-psnc	XFS	Non presente
brotzu-lbl1-psn	XFS	Non presente
brotzu-lbl2-psn	XFS	Non presente

Tabella 232 – Composizione Storage ARNAS

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.9.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
brotvm-app-san1-psn	10.77.13.2	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.13.0/27	N/A
brotvm-app-san2-psn	10.77.13.3	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.13.0/27	N/A

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
brotvm-app-san3-psnc	10.77.13.4	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.13.0/27	N/A
brotvm-app-san4-psnc	10.77.13.5	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.13.0/27	N/A
VIP ARNAS	10.77.12.252	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.12.224/27	N/A
brotzu-lbl1-psn	10.77.12.226	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.12.224/27	N/A
brotzu-lbl2-psn	10.77.12.227	PSN Industry Standard HA – Ambiente ARNAS - TGU servizio PSN02838744	10.77.12.224/27	N/A

Tabella 233 – Piano di indirizzamento ARNAS

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.9.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
brotvm-app-san1-psn	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----	Servizi Applicativi	NO	ASK DEV	Open Source
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/TEST/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/TEST/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181				

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
brotvm-app-san2-psn	Tomcat home directory: /opt/eliot/TEST/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----	Servizi Applicativi	NO	ASK DEV	Open Source
	Tomcat home directory: /opt/eliot/TEST/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35 Tomcat version: 8.0.35 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33_PREPROD Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181 -----				
	Tomcat home directory: /opt/eliot/PROD/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181				
brotvm-app-san3-psnc	Tomcat	Servizi Applicativi	NO	ASK DEV	Open Source
brotvm-app-san4-psnc	Tomcat	Servizi Applicativi	NO	ASK DEV	Open Source
brotzu-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
brotzu-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (Sardegna IT)

Tabella 234 – Software installato ARNAS

4.9.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
brotvm-app-san1-psn	Tomcat	8	Open Source
brotvm-app-san2-psn	Tomcat	8	Open Source
brotvm-app-san3-psnc	Tomcat	8	Open Source
brotvm-app-san4-psnc	Tomcat	8	Open Source

Tabella 235 – Web server ARNAS

4.9.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	AOBPDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 236 – Database server ARNAS

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.9.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISA, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 237 - Server DNS ARNAS

4.9.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 238 – Storage condivisi ARNAS

4.9.2.5 Networking

4.9.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.9.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Domain	Redirect to (URL/UriPath)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://eliot-aobpreproduzione.sisar.asl	http://eliot-aobpreproduzione.sisar.asl/WDOEliot	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2:8086 10.77.13.3:8086
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://eliot-aobtest.sisar.asl	http://eliot-aobtest.sisar.asl/WDOEliot	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2:8087 10.77.13.3:8087
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://areas-brot.sisar.asl/areas	http://areas-brot.sisar.asl/areas	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2:8080 10.77.13.3:8080 10.77.13.2:8180 10.77.13.3:8180
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://eliot-aob.sisar.asl	http://eliot-aob.sisar.asl/WDOEliot	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2:8090 10.77.13.3:8090
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://soweb-brot.sisar.asl/		brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2:8280 10.77.13.3:8280

brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	http://areasservizibrot.sisar.asl	http://areasservi zibrot.sisar.asl/ar easserv	brotvm-esb- san1 brotvm-esb- san2	10.77.13.4:8780 10.77.13.5:8780
brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	80	healthcheck	/LBLHealthCheck		localhost:5991

Tabella 239 – Bilanciamento ARNAS

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 240 – Tipo keepalive ARNAS

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 241 – Tipo persistenza sessione ARNAS

Tipologia balancing

Bilanciamento
Least Connection

Tabella 242 – Tipologia balancing ARNAS

Tipo Domain Enable

Domain Enable
True

Tabella 243 – Domain enable ARNAS

Type

Type
Adaptive

Tabella 244 – Type ARNAS

4.9.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Tabella 245 – Reverse proxy ARNAS

4.9.2.5.4 Flussi e Accessibilità

4.9.2.5.4.1 Flussi interni

4.9.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80443		Integrazione PUA - PUA

Tabella 246 – Flussi SIOAAP ARNAS

4.9.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn	10.77.13.2 10.77.13.3	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

Tabella 247 – Flussi SIOAAP – Connessioni a DB ARNAS

4.9.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer ARNAS	brotzu-lbl1-psn brotzu-lbl2-psn	10.77.12.226 10.77.12.227	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server ARNAS	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 248 – Flussi DNS ARNAS

4.9.2.5.4.2 Flussi esterni

4.9.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-brot.sisar.asl	brotvm-app-san1-psn	10.77.13.2 10.77.13.3	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integrazione con COT

	brotvm- app-san2- psn									
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	interoperabilita.i nail.it	interoperabilita.i nail.it	93.147.161.1 49		TCP	443		PS Inail integrazione
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80 443		E- prescription integrazione
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazione
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	protocollo.sisar.a sl	protocollo.sisar.a sl	10.3.66.40		TCP	80 443		Protocollo Integrazione
areas- brot.sisar.asl	brotvm- app-san1- psn brotvm- app-san2- psn	10.77.13.2 10.77.13.3	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integrazione Picasso (ADT-EDF)

Tabella 249 – Flussi SIOAAP ARNAS

4.9.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
TBD (PaaS DB)	TBD (Pa	Listener EXACS	db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD	Listener EXACS	db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 250 – Flussi SIOAAP – Connessioni a DB ARNAS

4.9.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocolo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areas-brot.sisar.asl	areas-brot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster-okd.sisar.asl	10.3.61.54	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster-okd.sisar.asl	10.3.61.55	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster-okd.sisar.asl	10.3.61.56	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster-okd.sisar.asl	10.3.61.57	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster-okd.sisar.asl	10.3.61.58	areasservizibrot.sisar.asl	areasservizibrot.sisar.asl	10.77.12.252		TCP	80443		INTEGRAZIONE PICASSO

Tabella 251 – Flussi PICASSO ARNAS

4.9.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-04.cluster - okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.cluster - okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster - okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster - okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster - okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster - okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

Tabella 252 - Flussi PICASSO – Connessioni a DB ARNAS

4.9.2.5.4.2.5 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
	brotvm-app-san1-psn	10.77.13.2			10.77.13.5			5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot
	brotvm-app-san2-psn	10.77.13.3			10.77.13.5			5050	R/W	servizio http esposto da spagic all'oe; flusso:PrintEtichettaEliot

	brovm-esb-san2	10.77.13.5			10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: PrintEtichettaEliot
	brovm-esb-san2				10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: CambioStato
	brovm-esb-san2				10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: CambioStatoDettaglio_EL IOT
	brovm-esb-san2	10.77.13.5			10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: CambioStatoDettaglio
	brovm-esb-san2	10.77.13.5							R/W	tipo: http da spagic a WS; flusso: Siemens_CambioStato
	brovm-esb-san2	10.77.13.5							R/W	tipo: http da spagic a WS; flusso: AOB_OE_TO_SIE_RIS
	brovm-esb-san2	10.77.13.5			10.77.13.2			8080	R/W	tipo: http da spagic a WS; flusso: SendRichiesteToRad
	brovm-esb-san2	10.77.13.5			10.77.13.2			8080	R/W	tipo: http da spagic a WS; flusso: SendRichiesteToRad
	brovm-esb-san2	10.77.13.5							R/W	tipo: http da spagic a WS; flusso: GetRefertoRisSiemens
	brovm-esb-san2	10.77.13.5			10.77.13.2			8080	R/W	tipo: http da spagic a WS; flusso: Radiologia_Evnt1
	brovm-esb-san2	10.77.13.5			10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: OE_TrasfusionaleReperisc iRisultatiHL7

	brovm-esb-san2	10.77.13.5			10.77.13.2			8180	R/W	tipo: http da spagic a WS; flusso: TrasfSendRichiestaHL7
	brovm-esb-san1	10.77.13.4			10.77.13.2			8080	R/W	tipo: http da spagic a WS; flusso: ApDedalusToOrderEntry
	brovm-esb-san2	10.77.13.5			10.77.13.3			8180	R/W	tipo: http da spagic a WS; flusso: orderEntryToAP
	brovm-esb-san1	10.77.13.4			10.77.13.2			8080	R/W	tipo: http da spagic a WS; flusso: UpdDatiSangue
	brovm-esb-san1	10.77.13.4						1521	R/W	Tutti i flussi
	brovm-esb-san2	10.77.13.5						1521	R/W	Tutti i flussi

Tabella 253 – Flussi SPAGIC ARNAS

4.9.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://eliot-aobpreproduzione.sisar.asl	10.77.12.252	Brovm-app-san1 Brovm-app-san2	10.77.13.2 10.77.13.3	HTTP	8086		no
http://eliot-aobtest.sisar.asl	10.77.12.252	Brovm-app-san1 Brovm-app-san2	10.77.13.2 10.77.13.3	HTTP	8087		no
http://areas-brot.sisar.asl/areas	10.77.12.252	Brovm-app-san1 Brovm-app-san2	10.77.13.2 10.77.13.3	HTTP	8080 8180		no

Endpoint pubblico / esterno	VIP	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://eliot-aob.sisar.asl	10.77.12.252	Brotvm-app-san1 Brotvm-app-san2	10.77.13.2 10.77.13.3	HTTP	8090		no
http://soweb-brot.sisar.asl/	10.77.12.252	Brotvm-app-san1 Brotvm-app-san2	10.77.13.2 10.77.13.3	HTTP	8280		no
http://areasservizibrot.sisar.asl	10.77.12.252	brotvm-esb-san1 brotvm-esb-san2	10.77.13.4 10.77.13.5	HTTP	8780		no
http://integrazionibrot.sisar.asl/demone	10.77.12.252	brotvm-esb-san1 brotvm-esb-san2	10.77.13.4 10.77.13.5	HTTP	8780		no

Tabella 254 – Accessi esterni/interni ARNAS

4.9.2.5.6 Sicurezza

4.9.2.5.7 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale.

4.9.2.5.8 Certificati SSL

Portale non esposto su internet.

4.9.2.5.9 Regole Firewall

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.66.7.54 10.66.7.132	93.39.83.53	HTTPS	TCP	443	Flussi Applicativi SIOAAP - INTEGRAZIONE CON COT
10.66.7.54 10.66.7.132	89.97.59.144	HTTPS	TCP	443	Flussi Applicativi SIOAAP -MD. LEG. vs INPS
10.66.7.54 10.66.7.132	93.147.161.149	HTTPS	TCP	443	Flussi Applicativi SIOAAP -PS Inail integrazione

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.66.7.54 10.66.7.132	10.39.250.12	HTTPS	TCP	443	Flussi Applicativi SIOAAP - PS Inail Integrazione
10.66.7.54 10.66.7.132	10.3.66.140	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - E- prescription integr.
10.66.7.54 10.66.7.132	10.3.66.40	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - EDF integrazione Protocollo Integrazione
10.66.7.54 10.66.7.132	10.193.1.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.250.61.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.160.151.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.96.61.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.128.101.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.3.99.23	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.80.61.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.66.1.20	HTTP HTTPS	TCP	80 443	Flussi Applicativi SIOAAP - Integr. PUA - PUA
10.66.7.54 10.66.7.132	10.66.7.140 10.66.7.141 10.66.7.142		TCP	1521	Flussi Applicativi SIOAAP - database sioaap (non presente in doc SardegnaIT)
10.66.7.140 10.66.7.141 10.66.7.142	10.3.67.167 10.3.67.168 10.3.67.169		TCP	1521	Flussi Applicativi SIOAAP - db_link AMC (non presente in doc SardegnaIT)

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.66.7.140 10.66.7.141 10.66.7.142	10.3.69.118 10.3.69.119 10.3.69.120		TCP	1521	Flussi Applicativi SIOAAP - db_link CUPWEB (non presente in doc SardegnaIT)
10.66.7.54 10.66.7.132	10.3.61.9		TCP	1521	Flussi Applicativi SIOAAP - integr Picasso (ADT-EDF) (non presente in doc SardegnaIT)
10.77.13.2	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.13.3	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.13.4	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.13.5	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.12.226	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.12.227	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN
10.77.13.6	10.77.2.60 10.77.2.61		TCP/UDP	53	from ARNAS to DNS CRESSAN

Tabella 255 – Regole firewall ARNAS

4.9.2.6 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.9.2.7 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza

Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati

nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
- WORM Protection:
 - Funzionalità della tecnologia di riferimento (Commvault) di WORM (Write Only Read Multiple) che si integra con le medesime funzionalità sullo storage di riferimento del repository;
 - La tecnologia di riferimento (Commvault) blocca i dati di backup da modifiche casuali non autorizzate e previene la modifica o l'eliminazione dei dati di backup intenzionale (I dati di backup saranno cancellati solo quando saranno state raggiunte le retention applicate);
 - Nessun amministratore del backup potrà cancellare i dati di backup non scaduti;
 - La tecnologia di riferimento (Commvault) convalida l'integrità dei dati durante il backup e durante le operazioni di copia dei dati. Quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul client di origine e

archiviati con il backup. Quando si copiano i dati, le firme (checksum CRC) vengono utilizzate per convalidare i blocchi di dati durante l'operazione di copia.

- Ransomware Protection:
 - Funzionalità Commvault di Ransomware protection;
 - I dati di backup sono bloccati e possono essere modificati solo dai processi della tecnologia di riferimento (Commvault);
 - Qualsiasi ransomware, applicazione o utente che tenti di eliminare, o modificare i dati di backup dal Media Agent (unico server che può accedere allo storage) riceverà una segnalazione di errore (catastrophic error dallo stack I/O del SO) a meno che non si tratti di un processo della tecnologia di riferimento (Commvault) autorizzato (modalità like SE-Linux).

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	I P	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
brotvm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
brotvm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
brotvm-app-san3-psnc		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
brotvm-app-san4-psnc		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
brotzu-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
brotzu-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> Backup Full 1 volta a settimana; Backup incrementale 1 volta al giorno; Backup Archivelog ogni 2 ore. 	30 gg

Tabella 256 – Policy di backup ARNAS

4.9.2.8 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.10 AOU CAGLIARI

4.10.1 Architettura

L'architettura applicativa, rappresentata in Figura 11, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

La stessa implementazione del servizio di database Oracle menzionato sarà utilizzata sia dal tenant ALS 8 di Cagliari che dal tenant AOUC, in continuità con l'architettura attualmente in esercizio on-premise. Non è possibile dedicare un DBMS Oracle ad uso esclusivo del tenant AOUC a causa delle seguenti problematiche:

- È necessario stimare e realizzare un intervento per estendere l'interoperabilità anagrafica e adeguare le integrazioni dei sistemi dipartimentali coinvolti con sistemi esterni.
- Si verificherebbe una perdita di univocità dell'ID Paziente dipartimentale nei confronti di sistemi di terze parti, con conseguenti gravi disservizi e rischi di anomalie sui dati.
- I sistemi di terze parti non sono predisposti a ricevere richieste o inviare aggiornamenti di stato a endpoint diversi.
- Le attuali interazioni tramite DBLink richiederebbero una reingegnerizzazione delle integrazioni.
- Non sarebbe possibile effettuare la migrazione di sicurezza inversa con Golden Gate, precludendo un piano di rollback in caso di esito migratorio non conforme alle previsioni.
- La pianificazione della migrazione subirebbe ritardi.

Pertanto, ASL 8 di Cagliari e AOUC condivideranno la stessa infrastruttura DBMS Oracle su Exadata, pur disponendo di infrastrutture IaaS Shared HA dedicate.

L'architettura di sicurezza, rappresentata in Figura 11, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSAN e tenant AOUC è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant AOUC, per mezzo della VRF.

Nel layer di FrontEnd sono presenti due bilanciatori (aouca-lbl1-psn – aouca-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.10.1.1 Schema Logico

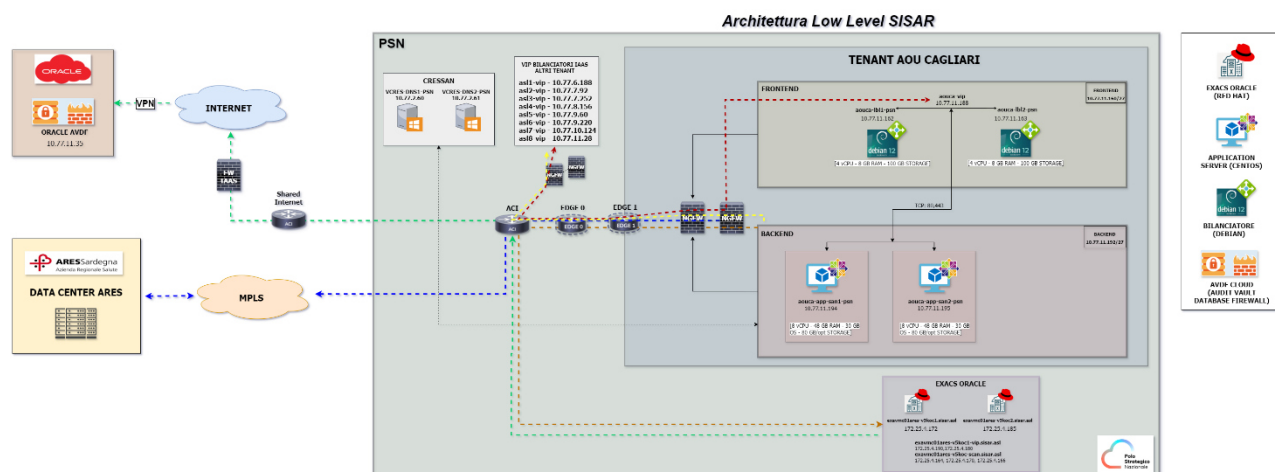


Figura 11 - Schema logico AOU CAGLIARI

4.10.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
aouca-app-san1-psn	AOU CA	Application	Application Server	Virtuale	No
aouca-app-san2-psn	AOU CA	Application	Application Server	Virtuale	No
aouca-vip-psn	AOUCA	Presentation	Virtual IP	Virtuale	No
aouca-lbl1-psn	AOU CA	Presentation	Balancer	Virtuale	No
aouca-lbl2-psn	AOU CA	Presentation	Balancer	Virtuale	No
N/A	AOU CA	Data	Oracle Exadata Cloud at Service	Virtuale	No

Tabella 257 – Lista componenti AOU CAGLIARI

4.10.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

4.10.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.10.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
aouca-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
aouca-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
aouca-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
aouca-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 258 – Caratteristiche AOU CAGLIARI

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.10.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
aouca-app-san1-psn	8	48	OS 30GB - /opt 80GB	SSD
aouca-app-san2-psn	8	48	OS 30GB - /opt 80GB	SSD
aouca-lbl1-psn	4	8	100	SSD
aouca-lbl2-psn	4	8	100	SSD

Tabella 259 – Dimensionamento AOU CAGLIARI

4.10.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
anouca-app-san1-psn	XFS	Non presente
anouca-app-san2-psn	XFS	Non presente
anouca-lbl1-psn	XFS	Non presente
anouca-lbl2-psn	XFS	Non presente

Tabella 260 – Composizione storage AOU CAGLIARI

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.10.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
anouca-vip	10.77.11.188	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.11.160/27	N/A
anouca-app-san1-psn	10.77.11.194	PSN Industry Standard HA – Ambiente AOU CA - TGU servizio PSN02838563	10.77.11.192/27	N/A
anouca-app-san2-psn	10.77.11.195	PSN Industry Standard HA – Ambiente AOU CA - TGU servizio PSN02838563	10.77.11.192/27	N/A
anouca-lbl1-psn	10.77.11.162	PSN Industry Standard HA – Ambiente AOU CA - TGU servizio PSN02838563	10.77.11.160/27	N/A
anouca-lbl2-psn	10.77.11.163	PSN Industry Standard HA – Ambiente AOU CA - TGU servizio PSN02838563	10.77.11.160/27	N/A

Tabella 261 – Piano di Indirizzamento AOU CAGLIARI

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.10.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
aouca-app-san1-psn	Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181	Servizi Applicativi	NO	ASK DEV	Open Source
	----- Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_aouca Tomcat version: 8.0.35 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181				

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
aouca-app-san2-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_asl8 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_24</p>	Servizi Applicativi	NO	ASK DEV	Open Source
aouca-lbl1-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (SardegnaIT)
aouca-lbl2-psn	Oplon OSA 10.10.003	Load Balancer – Reverse Proxy	NO	NO	In capo a DEC (SardegnaIT)

Tabella 262 – Software Installato AOU CAGLIARI

4.10.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
auca-app-san1-psn	Tomcat	8	Open Source
auca-app-san2-psn	Tomcat	8	Open Source

Tabella 263 – Web Server AOU CAGLIARI

4.10.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	AOUCAPDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 264 – Database server AOU CAGLIARI

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.10.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISA, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 265 – DNS

4.10.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 266 – Storage condivisi

4.10.2.5 Networking

4.10.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.10.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Hostname/FQDN/URL	Tipologia balancing (LC, RR, ...)	Persistenza sessione	Keepalive (TCP\URL,...)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
aouca-lbl1-psn aouca-lbl2-psn	10.77.11.162 10.77.11.163	80	http://areas-aouca.sisar.asl/areas	Least Connection	In base all'indirizzo IP di origine	TCP	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.194 10.77.11.195
aouca-lbl1-psn aouca-lbl2-psn	10.77.11.2 10.77.11.3	80	http://soweb-aouca.sisar.asl/	Least Connection	In base all'indirizzo IP di origine	TCP	aouca-app-san1-psn	10.77.11.194

Tabella 267 – Bilanciamento AOU CAGLIARI

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 268 – Tipo keepalive AOU CAGLIARI

Tipo persistenza sessione

Persistenza di Sessione
In base all'indirizzo IP di origine

Tabella 269 – Tipo persistenza sessione AOU CAGLIARI

Tipologia balancing

Bilanciamento
Least Connection

Tabella 270 – Tipologia balancing AOU CAGLIARI

Tipo Domain Enable

Domain Enable
True

Tabella 271 – Tipologia domain enable AOU CAGLIARI

Type

Type
Adaptive

Tabella 272 – Type AOU CAGLIARI

4.10.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
10.77.11.162 10.77.11.163	10.77.11.260	aouca-lbl1-psn aouca-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl8.sardegna salute.it	Adaptive	true	<p>puaslar.sisar.asl:80/pua</p> <p>puaslar.sisar.asl:80/ras-sp</p>	redirect to LBL priv ASL8

Tabella 273 – Reverse Proxy AOU CAGLIARI

4.10.2.5.4 Flussi e Accessibilità

4.10.2.5.4.1 Flussi interni

4.10.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA

areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl7.sisar.asl	N/A	10.77.10.124	TCP	80 443		Integrazione PUA - PUA
areas- asl8.sisar.asl	aouca- app- san1-psn aouca- app- san2-psn	10.77.11.34 10.77.11.35	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl1.sisar.asl	asl1vm- app- san1-psn asl1vm- app- san2-psn	10.77.6.194 10.77.6.195	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl2.sisar.asl	asl2vm- app- san1-psn asl2vm- app- san2-psn	10.77.7.98 10.77.7.99	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl3.sisar.asl	asl3vm- app- san1-psn asl3vm- app- san2-psn	10.77.8.2 10.77.8.3	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA

areas- asl4.sisar.asl	asl4vm- app- san1-psn asl4vm- app- san2-psn	10.77.8.262 10.77.8.263	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl5.sisar.asl	asl5vm- app- san1-psn asl5vm- app- san2-psn	10.77.9.66 10.77.9.66	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl6.sisar.asl	asl6vm- app- san1-psn asl6vm- app- san2-psn	10.77.9.226 10.77.9.227	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- asl7.sisar.asl	asl7vm- app- san1-psn asl7vm- app- san2-psn	10.77.10.13 0 10.77.10.13 1	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas- brot.sisar.asl	brotvm- app- san1-psn brotvm- app- san2-psn brotvm- app- san3- psnc brotvm- app- san4- psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA

Tabella 274 – Flussi SIOAAP AOU CAGLIARI

4.10.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas- asl8.sisar.asl	aouca- app-san1- psn aouca- app-san2- psn	10.77.11.34 10.77.11.35	Oracle ExaCS	TBD	Listener EXACS	TCP	152 1		Database Sioaap

Tabella 275 – Flussi SIOAAP – Connessioni a DB AOU CAGLIARI

4.10.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer AOUC	aouca-lbl1-psn aouca-lbl2-psn	10.77.11.162 10.77.11.163	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server AOUC	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.194 10.77.11.195	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 276 – Flussi DNS AOU CAGLIARI

4.10.2.5.4.2 Flussi esterni

4.10.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	cot.aressardegna.it	cot.aressardegna.it	93.39.83.53		TCP	443		Integrazione con COT
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	spcoop.inps.it	spcoop.inps.it	89.97.59.144		TCP	443		MD. LEG. vs INPS
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-	10.77.11.34 10.77.11.35	interoperabilita.inail.it	interoperabilita.inail.it	93.147.16.1149		TCP	443		PS Inail integrazione

	san2-psn									
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	pddras	pddras	10.39.250.12		TCP	444		PS Inail Integrazione
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.140		TCP	80443		E-prescription integrazione
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80443		EDF integrazione
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80443		Protocollo Integrazione
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	vip-picasso-cressan.sisar.asl	vip-picasso-cressan.sisar.asl	tutti i nodi		TCP	443		Integrazione Picasso (ADT-EDF)

Tabella 277 – Flussi SIOAAP AOU CAGLIARI

4.10.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC

Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 278 – Flussi SIOAAP – Connessioni a DB AOU CAGLIARI

4.10.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.clusterr-okd.sisar.asl	10.3.61.50	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.clusterr-okd.sisar.asl	10.3.61.51	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.clusterr-okd.sisar.asl	10.3.61.52	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.clusterr-okd.sisar.asl	10.3.61.53	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-05.clusterr-okd.sisar.asl	10.3.61.54	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.clusterr-okd.sisar.asl	10.3.61.55	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.clusterr-okd.sisar.asl	10.3.61.56	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.clusterr-okd.sisar.asl	10.3.61.57	areas-aouca.sisar.asl	areas-aouca.sisar.asl	10.77.11.188		TCP	80443		INTEGRAZIONE PICASSO

	r- okd.sisar. asl									
Worker Node Picasso	worker- node- 09.cluste r- okd.sisar. asl	10.3. 61.58	areas- aouca.sisar. asl	areas- aouca.sisar.asl	10.77.11.188		TCP	80 44 3		INTEGRAZION E PICASSO

Tabella 279 – Flussi PICASSO AOU CAGLIARI

4.10.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostnam e \ DNS destinati on	IP destination	Tipo sistem a estern o (SaaS, on prem ,...)	Protocol lo \ tecnolog ia	Port a	Rea d \ writ e	Contenuto flusso
Worker Node Picasso	worker- node- 01.cluster- okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 02.cluster- okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 03.cluster- okd.sisar.asl	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 04.cluster- okd.sisar.asl	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 05.cluster- okd.sisar.asl	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 06.cluster- okd.sisar.asl	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 07.cluster- okd.sisar.asl	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 08.cluster- okd.sisar.asl	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 09.cluster- okd.sisar.asl	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO

Tabella 280 – Flussi PICASSO – Connessioni a DB AOU CAGLIARI

4.10.2.5.5 Accessi esterni/interni

Endpoint pubblico / esterno	VIP (OPLON)	Hostname	IP	Protocollo \ tecnologia	Porta	Descrizione	Pubblico si/no
http://areas-aouca.sisar.asl/areas	10.77.11.162 10.77.11.163	aouca-app-san1-psn	10.77.11.194			ASSISTENZA SPECIALISTICA AMBULATORIALE PRONTO SOCCORSO RICOVERO ORDINARIO PER ACUTI DAY SURGERY DAY HOSPITAL	
http://areas-aouca.sisar.asl/areas	10.77.11.162 10.77.11.163	aouca-app-san2-psn	10.77.11.195			ASSISTENZA SPECIALISTICA AMBULATORIALE PRONTO SOCCORSO RICOVERO ORDINARIO PER ACUTI DAY SURGERY DAY HOSPITAL	
http://soweb-aouca.sisar.asl/	10.77.11.162 10.77.11.163	aouca-app-san1-psn	10.77.11.194			DAY SURGERY	

Tabella 281 – Accessi esterni/interni AOU CAGLIARI

4.10.2.6 Sicurezza

4.10.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale.

4.10.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardagnasalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui proprio dispositivi.

4.10.2.6.3 Regole Firewall

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.11.194	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU CAGLIARI to DNS CRESSAN

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.11.195	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU CAGLIARI to DNS CRESSAN
10.77.11.162	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU CAGLIARI to DNS CRESSAN
10.77.11.163	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU CAGLIARI to DNS CRESSAN

Tabella 282 – Regole firewall AOU CAGLIARI

4.10.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.10.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:

- Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
- WORM Protection:
 - Funzionalità della tecnologia di riferimento (Commvault) di WORM (Write Only Read Multiple) che si integra con le medesime funzionalità sullo storage di riferimento del repository;
 - La tecnologia di riferimento (Commvault) blocca i dati di backup da modifiche casuali non autorizzate e previene la modifica o l'eliminazione dei dati di backup intenzionale (I dati di backup saranno cancellati solo quando saranno state raggiunte le retention applicate);
 - Nessun amministratore del backup potrà cancellare i dati di backup non scaduti;
 - La tecnologia di riferimento (Commvault) convalida l'integrità dei dati durante il backup e durante le operazioni di copia dei dati. Quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul client di origine e archiviati con il backup. Quando si copiano i dati, le firme (checksum CRC) vengono utilizzate per convalidare i blocchi di dati durante l'operazione di copia.
 - Ransomware Protection:
 - Funzionalità Commvault di Ransomware protection;
 - I dati di backup sono bloccati e possono essere modificati solo dai processi della tecnologia di riferimento (Commvault);
 - Qualsiasi ransomware, applicazione o utente che tenti di eliminare, o modificare i dati di backup dal Media Agent (unico server che può accedere allo storage) riceverà una segnalazione di errore (catastrophic error dallo stack I/O del SO) a meno che non si tratti di un processo della tecnologia di riferimento (Commvault) autorizzato (modalità like SE-Linux).

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice:

da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	I P	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
aouca-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouca-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouca-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouca-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup ArchiveLog ogni 2 ore. 	30 gg

Tabella 283 – Policy di backup AOU CAGLIARI

4.10.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l'Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo

progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l'Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.11 AOU SASSARI

4.11.1 Architettura

L'architettura applicativa, rappresentata in Figura 12, è suddivisa nei 2 layer di FrontEnd e BackEnd un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

La stessa implementazione del servizio di database Oracle menzionato sarà utilizzato sia dal tenant ALS 1 di Sassari che dal tenant AOUSS, in continuità con l'architettura attualmente in esercizio on-premise. Non è possibile dedicare un DBMS Oracle ad uso esclusivo del tenant AOUSS a causa delle seguenti problematiche:

- È necessario stimare e realizzare un intervento per estendere l'interoperabilità anagrafica e adeguare le integrazioni dei sistemi dipartimentali coinvolti con sistemi esterni.
- Si verificherebbe una perdita di univocità dell'ID Paziente dipartimentale nei confronti di sistemi di terze parti, con conseguenti gravi disservizi e rischi di anomalie sui dati.
- I sistemi di terze parti non sono predisposti a ricevere richieste o inviare aggiornamenti di stato a endpoint diversi.
- Le attuali interazioni tramite DBLink richiederebbero una reingegnerizzazione delle integrazioni.
- Non sarebbe possibile effettuare la migrazione di sicurezza inversa con Golden Gate, precludendo un piano di rollback in caso di esito migratorio non conforme alle previsioni.
- La pianificazione della migrazione subirebbe ritardi.

Pertanto, ASL 1 di Sassari e AOUSS condivideranno la stessa infrastruttura DBMS Oracle su Exadata, pur disponendo di infrastrutture IaaS Shared HA dedicate.

L'architettura di sicurezza, rappresentata in Figura 12, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra il tenant CRESSAN e tenant AOUISS è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge, mentre la comunicazione verso l'Exadata Cloud Service avviene attraverso i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server, presente nel layer del FrontEnd del Tenant AOUISS, per mezzo della VRF.

Nel layer di FrontEnd sono presenti due bilanciatori (aouss-lbl1-psn – aouss-lbl2-psn).

Nel layer di BackEnd sono presenti i server applicativi e il server Oracle Database Firewall che permette agli AVDF (Audit Vault Database Firewall) in Oracle Cloud di eseguire l'audit dei database e di monitorare le attività di rete dei database Oracle.

4.11.1.1.1 Schema Logico

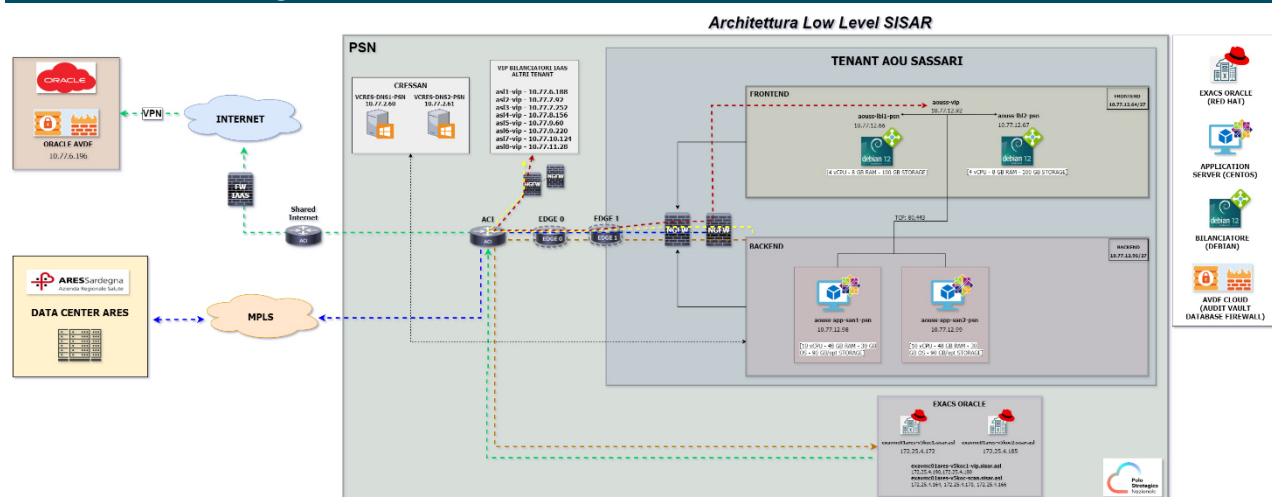


Figura 12 - Schema logico AOU SASSARI

4.11.1.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
aouss-app-san1-psn	AOU SS	Application	Application Server	Virtuale	No
aouss-app-san2-psn	AOU SS	Application	Application Server	Virtuale	No
aouss-vip-psn	AOU SS	Presentation	Virtual IP	Virtuale	No
aouss-lbl1-psn	AOU SS	Presentation	Balancer	Virtuale	No

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
aouss-lbl2-psn	AOU SS	Presentation	Balancer	Virtuale	No
N/A	AOU SS	Data	Oracle Exadata Cloud at Service	Virtuale	No

Tabella 284 – Lista componenti AOU SASSARI

4.11.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

4.11.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.11.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
aouss-app-san1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
aouss-app-san2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
aouss-lbl1-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm
aouss-lbl2-psn	vSphere 8.0, VCDA ≥ 10.3.x	VMWare	Debian	12 bookworm

Tabella 285 – Caratteristiche AOU SASSARI

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.11.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif Tabella Tipologia Storage)
aouss-app-san1-psn	10	48	OS 30GB - /opt 90GB	SSD
aouss-app-san2-psn	10	48	OS 30GB - /opt 90GB	SSD
aouss-lbl1-psn	4	8	100	SSD
aouss-lbl2-psn	4	8	100	SSD

Tabella 286 – Dimensionamento AOU SASSARI

4.11.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
aouss-app-san1-psn	XFS	Non presente
aouss-app-san2-psn	XFS	Non presente
aouss-lbl1-psn	XFS	Non presente
aouss-lbl2-psn	XFS	Non presente

Tabella 287 – Composizione storage AOU Sassari

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.11.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
aouss-vip	10.77.12.92	PSN Industry Standard HA – Ambiente ASL01 - TGU servizio PSN02838179	10.77.12.64/27	N/A
aouss-app-san1-psn	10.77.12.98	PSN Industry Standard HA – Ambiente AOU SS - TGU servizio PSN02838203	10.77.12.96/27	N/A

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
aouss-app-san2-psn	10.77.12.99	PSN Industry Standard HA – Ambiente AOU SS - TGU servizio PSN02838203	10.77.12.96/27	N/A
aouss-lbl1-psn	10.77.12.66	PSN Industry Standard HA – Ambiente AOU SS - TGU servizio PSN02838203	10.77.12.64/27	N/A
aouss-lbl2-psn	10.77.12.67	PSN Industry Standard HA – Ambiente AOU SS - TGU servizio PSN02838203	10.77.12.64/27	N/A

Tabella 288 – Piano di indirizzamento AOU SASSARI

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.11.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
aouss-app-san1-psn	Tomcat home directory: /opt/sian/apache-to Tomcat version: 8.0.39 JDK version: 1.8.0_181	Servizi Applicativi	NO	ASK DEV	Open Source
	----- Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_10				
	----- Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35-asl1 Tomcat version: 8.0.35 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	----- Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181				

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
aouss-app-san2-psn	Tomcat home directory: /opt/soweb/apache-t5-aouss Tomcat version: 8.0.35 JDK version: 1.8.0_181	Servizi Applicativi	NO	ASK DEV	Open Source
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181				
	Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181				
aouss-lbl1-psn	Oplon OSA 10.10.003	Load Balancer - Reverse Proxy	NO	NO	In capo al DEC (Sardegna IT)
aouss-lbl2-psn	Oplon OSA 10.10.003	Load Balancer - Reverse Proxy	NO	NO	In capo al DEC (Sardegna IT)

Tabella 289 – Software installato AOU SASSARI

4.11.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
aouss-app-san1-psn	Tomcat	8	Open Source
aouss-app-san2-psn	Tomcat	8	Open Source

Tabella 290 – Web Server AOU SASSARI

4.11.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	AOUSSPDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 291 – Database server AOU SASSARI

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.11.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller.

Hostname	IP	Tenant
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843

Tabella 292 - Server DNS AOU SASSARI

4.11.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 293 – Storage condivisi AOU SASSARI

4.11.2.5 Networking

4.11.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.11.2.5.2 Bilanciamento

Bilanciatore	IP Bilanciatore	Porte Bilanciatore	Hostname/FQDN/URL	Tipologia balancing (LC, RR, ...)	Persistenza sessione	Keepalive (TCP\URL,...)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
aouss-lbl1-psn aouss-lbl2-psn	10.77.12.66 10.77.12.67	80	http://areas-aouss.sisar.asl/areas	Least Connection	Con utilizzo di cookie (Arrowpoint cookie)	TCP	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.12.98:8081 10.77.12.98:8181 10.77.12.99:8081 10.77.12.99:8181
aouss-lbl1-psn aouss-lbl2-psn	10.77.12.66 10.77.12.67	80	http://soweb-aouss.sisar.asl	Least Connection	In base all'indirizzo IP di origine	TCP	asl1vm-app-san1-psn	10.77.12.99:8280

Tabella 294 – Bilanciamento AOU SASSARI

Tipo keepalive

Modalità di KeepAlive
TCP

Tabella 295 – Tipo keepalive AOU SASSARI

Tipo persistenza sessione

Persistenza di Sessione
Persistent Cookie

Tabella 296 – Tipo persistenza sessione AOU SASSARI

Tipologia balancing

Bilanciamento
Least Connection

Tabella 297 – Tipologia balancing AOU SASSARI

Tipo Domain Enable

Domain Enable
True

Tabella 298 – Tipo domain enable AOU SASSARI

Type

Type
Adaptive

Tabella 299 – Type AOU SASSARI

4.11.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URL Path	Note
10.77.12.66 10.77.12.67	10.77.12.64	aouss-lbl1-psn aouss-lbl2-psn	ADC_CUPWEB_PUB	ADC CupWeb Pubblico	puacomuni-asl1.sardegna salute.it	Adaptive	True	pu-a-sl1.sisar.asl:80/pua pu-a-sl1.sisar.asl:80/ras-sp	redirect to LBL priv ASL1

Tabella 300 – Reverse proxyReverse proxy

4.11.2.5.4 Flussi e Accessibilità

4.11.2.5.4.1 Flussi interni

4.11.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl2.sisar.asl	N/A	10.77.7.92	TCP	80443		Integrazione PUA - PUA

areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl3.sisar.asl	N/A	10.77.7.252	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl4.sisar.asl	N/A	10.77.8.256	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl5.sisar.asl	N/A	10.77.9.60	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl6.sisar.asl	N/A	10.77.9.220	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl7.sisar.asl	N/A	10.77.10.12 4	TCP	80 443		Integrazione PUA - PUA
areas-asl1.sisar.asl	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195	areas-asl8.sisar.asl	N/A	10.77.11.38	TCP	80 443		Integrazione PUA - PUA
areas-asl2.sisar.asl	asl2vm-app-san1-psn asl2vm-app-san2-psn	10.77.7.98 10.77.7.99	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl3.sisar.asl	asl3vm-app-san1-psn asl3vm-app-san2-psn	10.77.8.2 10.77.8.3	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl4.sisar.asl	asl4vm-app-san1-psn asl4vm-app-san2-psn	10.77.8.262 10.77.8.263	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA
areas-asl5.sisar.asl	asl5vm-app-san1-psn asl5vm-app-san2-psn	10.77.9.66 10.77.9.66	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80 443		Integrazione PUA - PUA

areas-asl6.sisar.asl	asl6vm-app-san1-psn asl6vm-app-san2-psn	10.77.9.226 10.77.9.227	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl7.sisar.asl	asl7vm-app-san1-psn asl7vm-app-san2-psn	10.77.10.130 10.77.10.131	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-asl8.sisar.asl	aouca-app-san1-psn aouca-app-san2-psn	10.77.11.34 10.77.11.35	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
areas-brot.sisar.asl	brotvm-app-san1-psn brotvm-app-san2-psn brotvm-app-san3-psnc brotvm-app-san4-psnc	10.77.13.2 10.77.13.3 10.77.13.4 10.77.13.5	areas-asl1.sisar.asl	N/A	10.77.6.188	TCP	80443		Integrazione PUA - PUA
Load Balancer ASL1	aouss-lbl1-psn aouss-lbl2-psn	10.77.6.162 10.77.6.163	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		
Application Server ASL1	asl1vm-app-san1-psn asl1vm-app-san2-psn	10.77.6.194 10.77.6.195 10.77.6.196	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		

Tabella 301 – Flussi SIOAAP AOU SASSARI

4.11.2.5.4.1.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
areas-asl1.sisar.asl	asl1vm-app-san1-psn	10.77.6.194	Oracle ExaCS	TBD	Listener EXACS	TCP	1521		Database Sioaap

	asl1vm- app-san2- psn	10.77.6.19 5							
--	-----------------------------	-----------------	--	--	--	--	--	--	--

Tabella 302 – Flussi SIOAAP – Connessioni a DB AOU SASSARI

4.11.2.5.4.1.3 Flussi DNS

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Load Balancer AO USS	aouss-lbl1- psn aouss-lbl2- psn	10.77.12.66 10.77.12.67	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan
Application Server AO USS	aouss-app- san1-psn aouss-app- san2-psn	10.77.12.98 10.77.12.99	DNS Server	VCRES-DNS1-PSN VCRES-DNS2-PSN	10.77.2.60 10.77.2.61	TCP UDP	53		DNS Cressan

Tabella 303 – Flussi DNS AOU SASSARI

4.11.2.5.4.2 Flussi esterni

4.11.2.5.4.2.1 Flussi SIOAAP

Sistema source	Hostna me \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destinatio n	Tipo siste ma ester no (SaaS , on prem , ...)	Protoc ollo \ tecnol ogia	Por ta	Rea d \ wri te	Contenuto flusso
areas- asl1.sisar.asl	asl1vm- app- san1- psn asl1vm- app- san2- psn	10.77.6. 194 10.77.6. 195	cot.aressardegna.it	cot.aressardegna.it	93.39.83.5 3		TCP	443		Integrazione con COT
areas- asl1.sisar.asl	asl1vm- app- san1- psn asl1vm- app- san2- psn	10.77.6. 194 10.77.6. 195 10.77.6. 196	spcoop.inps.it	spcoop.inps.it	89.97.59.1 44		TCP	443		MD. LEG. vs INPS

areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	interoperabilita.inai l.it	interoperabilita.inai l.it	93.147.16 1.149		TCP	443		PS Inail integrazione
areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	pddras	pddras	10.39.250. 12		TCP	443		PS Inail Integrazione
areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	cupweb.sisar.asl	cupweb.sisar.asl	10.3.66.14 0		TCP	80 443		E-prescription integrazione
areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	areas.sisar.asl	areas.sisar.asl	10.3.66.40		TCP	80 443		EDF integrazione
areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	protocollo.sisar.asl	protocollo.sisar.asl	10.3.66.40		TCP	80 443		Protocollo Integrazione
areas- asl1.sisar.asl	asl1vm -app- san1- psn asl1vm -app- san2- psn	10.77.6. 194 10.77.6. 195	vip-picasso- cressan.sisar.asl	vip-picasso- cressan.sisar.asl	tutti i nodi		TCP	443		Integrazione Picasso (ADT-EDF)

Tabella 304 – Flussi SIOAAP AOU SASSARI

4.11.2.5.4.2.2 Flussi SIOAAP – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Oracle ExaCS	TBD		db_link AMC	cluamc-scan.sisar.asl	Listener EXACS		TCP	1521		db_link AMC
Oracle ExaCS	TBD		db_link CUPWEB	cludcupweb-scan.sisar.asl	Listener EXACS		TCP	1521		db_link CUPWEB
vcres-monitorps	vcres-monitorps	10.3.67.233	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		talend - monitor PS

Tabella 305 – Flussi SIOAAP – Connessioni a DB AOU SASSARI

4.11.2.5.4.2.3 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster-okd.sisar.asl	10.3.61.50	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster-okd.sisar.asl	10.3.61.51	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster-okd.sisar.asl	10.3.61.52	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-04.cluster-okd.sisar.asl	10.3.61.53	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO

Worker Node Picasso	worker-node-05.cluster - okd.sisar.asl	10.3.61.54	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-06.cluster - okd.sisar.asl	10.3.61.55	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-07.cluster - okd.sisar.asl	10.3.61.56	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-08.cluster - okd.sisar.asl	10.3.61.57	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-09.cluster - okd.sisar.asl	10.3.61.58	areas-aouss.sisar.asl	areas-aouss.sisar.asl	10.77.12.92		TCP	80443		INTEGRAZIONE PICASSO

Tabella 306 – Flussi PICASSO AOU SASSARI

4.11.2.5.4.2.4 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem, ...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso
Worker Node Picasso	worker-node-01.cluster - okd.sisar.asl	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-02.cluster - okd.sisar.asl	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO
Worker Node Picasso	worker-node-03.cluster	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS		TCP	1521		INTEGRAZIONE PICASSO

	- okd.sisar. asl									
Worker Node Picasso	worker- node- 04.cluster - okd.sisar. asl	10.3.61. 53	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 05.cluster - okd.sisar. asl	10.3.61. 54	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 06.cluster - okd.sisar. asl	10.3.61. 55	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 07.cluster - okd.sisar. asl	10.3.61. 56	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 08.cluster - okd.sisar. asl	10.3.61. 57	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO
Worker Node Picasso	worker- node- 09.cluster - okd.sisar. asl	10.3.61. 58	Oracle ExaCS	TBD	Listener EXACS		TCP	152 1		INTEGRAZIONE PICASSO

Tabella 307 – Flussi PICASSO – Connessioni a DB AOU SASSARI

4.11.2.5.4.3 Flussi SPAGIC

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Tipo sistema esterno (SaaS, on prem ,...)	Protocollo \ tecnologia	Porta	Read \ write	Contenuto flusso

Tabella 308 – Flussi Spagic AOU SASSARI

4.11.2.6 Sicurezza

4.11.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale.

4.11.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegnasalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.11.2.6.3 Regole Firewall

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.12.98	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU SASSARI to DNS CRESSAN
10.77.12.99	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU SASSARI to DNS CRESSAN
10.77.12.66	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU SASSARI to DNS CRESSAN
10.77.12.67	10.77.2.60 10.77.2.61		TCP/UDP	53	from AOU SASSARI to DNS CRESSAN

Tabella 309 – Regole Firewall AOU SASSARI

4.11.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.11.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
- WORM Protection:
 - Funzionalità della tecnologia di riferimento (Commvault) di WORM (Write Only Read Multiple) che si integra con le medesime funzionalità sullo storage di riferimento del repository;
 - La tecnologia di riferimento (Commvault) blocca i dati di backup da modifiche casuali non autorizzate e previene la modifica o l'eliminazione dei dati di backup intenzionale (I dati di backup saranno cancellati solo quando saranno state raggiunte le retention applicate);
 - Nessun amministratore del backup potrà cancellare i dati di backup non scaduti;
 - La tecnologia di riferimento (Commvault) convalida l'integrità dei dati durante il backup e durante le operazioni di copia dei dati. Quando viene eseguito il backup dei dati per la prima volta, vengono calcolati i checksum CRC per ogni blocco di dati sul client di origine e archiviati con il backup. Quando si copiano i dati, le firme (checksum CRC) vengono utilizzate per convalidare i blocchi di dati durante l'operazione di copia.
- Ransomware Protection:
 - Funzionalità Commvault di Ransomware protection;

- I dati di backup sono bloccati e possono essere modificati solo dai processi della tecnologia di riferimento (Commvault);
- Qualsiasi ransomware, applicazione o utente che tenti di eliminare, o modificare i dati di backup dal Media Agent (unico server che può accedere allo storage) riceverà una segnalazione di errore (catastrophic error dallo stack I/O del SO) a meno che non si tratti di un processo della tecnologia di riferimento (Commvault) autorizzato (modalità like SE-Linux).

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	I P	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl1vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg

Hostname	I P	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
asl1vm-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
asl1vm-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouss-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouss-lbl2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 310 – Policy di backup AOU SASSARI

4.11.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

Per quanto attiene al servizio di Disaster Recovery (replica su altra region) si evidenzia che, in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzarlo in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

4.12

4.13 CRESSAN

4.13.1 Architettura

L'architettura applicativa, rappresentata in Figura 13, è suddivisa nei 2 layer di FrontEnd e BackEnd, un servizio database erogato dal Public Cloud PSN Managed tramite tecnologia Exadata Cloud Service di Oracle che prevede un'architettura sul PSN con un unico database pluggable PDB per ogni database contenitore CDB ed un servizio AVDF in Oracle Cloud.

L'architettura di sicurezza, rappresentata in Figura 13, è composta dai seguenti elementi:

NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;

WAF: Web Application Firewall per la mitigazione di eventuali attacchi di natura applicativa (L7);

EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La connettività fra i diversi tenant dipartimentali è attuata per mezzo di VPN IPSEC configurate sui Gateway Edge. In particolare, il Tenant CRESSAN, in virtù della sua designazione come contenitore di servizi centralizzati, svolgerà un ruolo di concentratore delle connessioni VPN verso gli altri tenant. Questo consentirà l'esposizione e la protezione delle applicazioni dei tenant dipartimentali, tramite il WAF presente nel Tenant CRESSAN. La comunicazione verso l'Exadata Cloud Service avviene invece tramite i VRF (Virtual Routing and Forwarding).

Una richiesta da MPLS viene inoltrata, dopo opportuna risoluzione DNS, verso il WAF del Tenant Cressan attraverso il Gateway EDGE del Tenant Cressan. Dopo essere stata analizzata ed ispezionata dal WAF, se ritenuta lecita, viene inoltrata dall'interfaccia external del WAF: la richiesta arriva al Real Server attraverso l'interfaccia Internal del WAF.

Il traffico internet proveniente dai portali **puacomuni**, presenti sui vari Tenant delle Asl, viene ridirezionato verso il Tenant Cressan, ispezionato dal WAF e reinoltrato verso il Tenant dell'Asl di destinazione.

Nel layer di BackEnd sono presenti i server applicativi dell'ambiente di test e i server DNS VCRES-DNS1-PSN e VCRES-DNS2-PSN.

4.13.1.1 Schema Logico

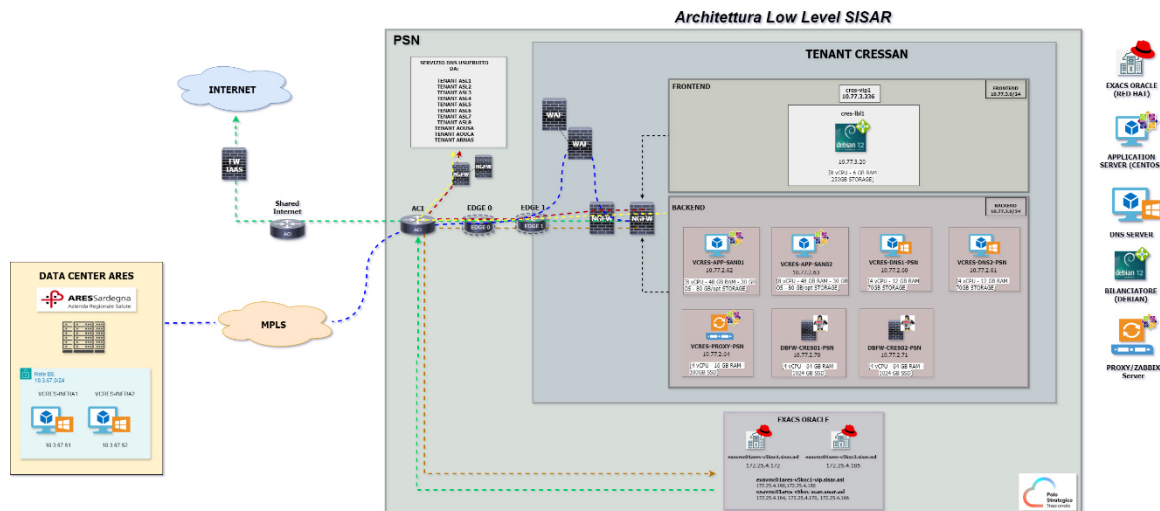


Figura 13 - Schema logico CRESSAN

4.13.1.2 Lista Componenti

Hostname	Data Center / Tenant cloud	Layer (Presentation / Application / Data)	Ruolo (Application server, balancer, etc)	Virtuale \ Fisico	Condiviso (SI/NO)
cres-vip1-psn	CRESSAN	Presentation	Virtual IP	Virtuale	No
cres-lbl1-psn	CRESSAN	Presentation	Virtual IP	Virtuale	No
VCRES-DNS1-PSN	CRESSAN	Application	DNS Server	Virtuale	No
VCRES-DNS2-PSN	CRESSAN	Application	DNS Server	Virtuale	No
vcres-app-san01-psn	CRESSAN	Application	Application Server	Virtuale	No
vcres-app-san02-psn	CRESSAN	Application	Application Server	Virtuale	No
N/A	CRESSAN	Data	Oracle Exadata Cloud at Service	Virtuale	No
vcres-proxy-psn	CRESSAN	Application	Proxy Server Zabbix	Virtuale	No

Tabella 311 – Lista componenti CRESSAN

4.13.2 Infrastruttura

L'infrastruttura a supporto della migrazione della piattaforma applicativa è basata su servizi Industry Standard e Public Cloud PSN Managed, con tipologie IaaS Shared HA e Licensed SQL e Oracle Hyperscaler Technology.

Il Polo Strategico Nazionale offre una Cloud Platform con la quale eroga i servizi Cloud alle amministrazioni finali. La Cloud Platform è concepita nativamente in High Availability tra almeno due Data Center (HA-Zone) costituenti una specifica Region. In particolare, sono attive due Region: Sud e Nord, la prima creata tra i DC di Acilia e Pomezia, la seconda tra i DC di Rozzano e Santo Stefano Ticino. Le HA-Zone di ogni Region sono interconnesse da un unico network layer in grado di consentire un modello di architettura flat che garantisca workload mobility ed alta affidabilità intrinseca delle soluzioni Cloud.

Nel caso specifico, il servizio IaaS Shared HA, istanziato per ARES Sardegna sui due DC della Region Sud di Acilia e Pomezia, consiste nella messa a disposizione di un'infrastruttura virtualizzata e condivisa, in cui non viene allocata alcuna risorsa ad uso esclusivo, basata su tecnologia VMWare.

Il servizio infrastrutturale viene erogato in Alta Affidabilità in modalità "stretched", in cui l'infrastruttura da migrare viene replicata in automatico nelle due HA-Zone della region Sud, con l'obiettivo di aumentare il livello di resilienza. L'opzione dell'Alta Affidabilità è da considerarsi come "managed" in carico al PSN, le Virtual Machine create nel Virtual Data Center (Tenant) risiederanno nella HA-Zone decisa in autonomia dalla funzione DRS (Distributed Resource Scheduler) di VMWare. Essendo una funzionalità nativa del servizio, non è possibile per un'Amministrazione governare la funzionalità dell'Alta Affidabilità, per esempio dalla Console Unica messa a disposizione dell'Amministrazione. In caso di fault di una HA-Zone, le Virtual Machine che vi risiedevano verranno accese in automatico sulla seconda HA Zone. Le Virtual Machine ripristinate subiranno un restart. Nel caso in cui tutta l'intera Region vada in fault allora in questo caso le Virtual Machine saranno spente fino a quando almeno un HA-Zone verrà ripristinato.

Esiste inoltre un'Alta Affidabilità nativa anche a livello di HA Zone, se un host che ospita una Virtual Machine diventa indisponibile allora verrà riaccesa su altri host disponibili.

Gli SLA associati al servizio IaaS Shared HA sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

4.13.2.1 Virtual Machine

Di seguito si fornisce il dettaglio delle VM atte ad ospitare la piattaforma applicativa.

4.13.2.1.1 Caratteristiche

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
cres-lbl1-psn	vSphere 8.0, VCDA \geq 10.3.x	VMWare	Debian	12 bookworm
VCRES-DNS1-PSN	vSphere 8.0, VCDA \geq 10.3.x	VMWare	Windows Server	2016 R2

Hostname	Cluster VMWare - DataCenter (se ambiente virtuale)	Tecnologia di virtualizzazione	Sistema Operativo	Versione SO
VCRES-DNS2-PSN	vSphere 8.0, VCD A ≥ 10.3.x	VMWare	Windows Server	2016 R2
vcres-app-san01-psn	vSphere 8.0, VCD A ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
vcres-app-san02-psn	vSphere 8.0, VCD A ≥ 10.3.x	VMWare	CentOS Linux	7.2.1511 (Core)
vcres-proxy-psn	vSphere 8.0, VCD A ≥ 10.3.x	VMWare	Ubuntu	24.0 LTS

Tabella 312 – Caratteristiche CRESSAN

Si precisa che il sistema operativo specificato per le virtual machines VCRES-DNS1-PSN e VCRES-DNS2-PSN è l'ultima versione compatibile con il functional levels di Active Directory, DNS e Domain Controller in ambiente on-premise.

L'amministrazione garantisce l'update, a versioni di SO e applicative non EoS, al più tardi entro sei mesi dalla sottoscrizione del contratto di utenza. Sino all'effettivo upgrade dei sistemi operativi impattati, PSN non potrà garantire la certificazione di tali sistemi nella propria infrastruttura, non avendo i requisiti compatibilità con i servizi di Industry standard. In tal senso, finché la PA non aggiornerà i propri Sistemi operativi, PSN provvederà al setup dei servizi impattati ma non potrà esser ritenuto responsabile di eventuali disservizi in termini di disponibilità (IQ 10) e presa in carico / risoluzione (IQ 16 e IQ17). Inoltre, PSN non potrà essere ritenuto responsabile di eventuali implicazioni di cyber sicurezza legate alle componenti applicative EoS.

Qualora vi fossero sistemi non compatibili con l'aggiornamento, l'effort stimato andrà comunque riconosciuto e consuntivato. Se la macchina non risulti tecnicamente migrabile, il relativo canone verrà escluso dalla consuntivazione annuale.

4.13.2.1.2 Dimensionamento

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif. Tabella Tipologia Storage)
cres-lbl1-psn	8	6	250	SSD
VCRES-DNS1-PSN	4	12	70 GB	SSD
VCRES-DNS2-PSN	4	12	70 GB	SSD
vcres-app-san01-psn*	8	48	OS 30GB - /opt 80GB	SSD
vcres-app-san02-psn*	8	48	OS 30GB - /opt 80GB	SSD

Hostname	CPU/vCPU (#)	RAM (GB)	Storage (GB)	Tipo Storage (rif. Tabella Tipologia Storage)
Audit-vault-1	32	128	2.048 GB	SSD
Audit-vault-2	32	128	2.048 GB	SSD
vcres-proxy-psn	4	16	100	SSD

Tabella 313 – Dimensionamento CRESSAN

* La modalità di migrazione sarà L&S e si procederà a clonare gli Application Server presenti nel dipartimentale ASL8.

4.13.2.1.3 Composizione Storage

Hostname	Elenco filesystem	NAS
cres-lbl1-psn	XFS	Non presente
VCRES-DNS1-PSN	NTFS	Non presente
VCRES-DNS2-PSN	NTFS	Non presente
vcres-app-san01-psn	XFS	Non presente
vcres-app-san02-psn	XFS	Non presente
vcres-proxy-psn	XFS	Non presente

Tabella 314 – Composizione storage CRESSAN

È stato condotto un approfondimento a livello storage sull'ambiente on-premise per verificare l'eventuale presenza di dischi non supportati, al fine di escludere problemi di compatibilità con il tool di migrazione VMware vCenter Converter Standalone 6.6.0.

Dall'analisi è emerso che nell'infrastruttura Hyper-V non sono presenti dischi in configurazione RAID, dischi ibridi GPT/MBR o dischi RDM, e che le macchine virtuali incluse nel processo di migrazione non utilizzano la crittografia sui dischi di sistema.

4.13.2.1.4 Piano di Indirizzamento

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
cres-vip1	10.77.0.236	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.0.0/24	N/A

Hostname	Indirizzo IP	Cloud Provider / Account	Rete	VLAN/VPC (*)
DBFW-CRES01-PSN	10.77.2.70	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
DBFW-CRES02-PSN	10.77.2.71	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
vcres-proxy-psn	10.77.2.64	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
cres-lbl1-psn	10.77.3.20	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.3.0/24	N/A
VCRES-DNS1-PSN	10.77.2.60	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
VCRES-DNS2-PSN	10.77.2.61	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
vcres-app-san01-psn	10.77.2.62	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A
vcres-app-san02-psn	10.77.2.63	PSN Industry Standard HA – Ambiente CRESSAN - TGU servizio PSN02837843	10.77.2.0/24	N/A

Tabella 315 – Piano di indirizzamento CRESSAN

(*) Nei contesti dei principali CSP, i concetti di VLAN/VPC sono ampiamente utilizzati per la gestione delle reti e la sicurezza dei servizi IaaS. Tuttavia, nell'implementazione del servizio IaaS Shared HA, questi concetti non sono direttamente applicabili sulle istanze di servizio rilasciate alle Amministrazioni finali.

4.13.2.1.5 Software Installato

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
vcres-app-san01-psn	<p>Tomcat home directory: /opt/sian/apache-tomcat-8.0.39 Tomcat version: 8.0.39 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_aouca Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181</p>	Servizi Applicativi	NO	ASK DEV	Open Source

Hostname	Software	Funzionalità fornita	Vincoli infrastruttura	Vincoli altri software \ librerie	Modello di licensing
vcres-app-san02-psn	<p>Tomcat home directory: /opt/soweb/apache-tomcat-8.0.35_asl8 Tomcat version: 8.0.35 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/medleg/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_121</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33 Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33b Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33c Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/tomcat/apache-tomcat-8.0.33d Tomcat version: 8.0.33 JDK version: 1.8.0_181</p> <p>-----</p> <p>Tomcat home directory: /opt/spresal/apache-tomcat-5.5.25/ Tomcat version: 5.5.25 JDK version: 1.6.0_24</p>	Servizi Applicativi	NO	ASK DEV	Open Source
cres-lbl1-psn	Oplon GDG 10.001	Load Balancer	NO	N/A	Open Source (Single Node)

Tabella 316 – Software installato CRESSAN

4.13.2.1.6 Web Server

Hostname	Tecnologia WebServer	Versione WebServer	Modello licensing
vcres-app-san01-psn	Tomcat	8	OpenSource
vcres-app-san02-psn	Tomcat	8	OpenSource

Tabella 317 – Web Server CRESSAN

4.13.2.2 Database Server

Hostname	Nome PDB	Tecnologia	Versione	Cluster \ single node	Risorse*	DATA*	FRA*	Modello licensing
exavmc01ares-v5koc1.sisar.asl exavmc01ares-v5koc2.sisar.asl	CRESTPDB	Oracle Exadata Cloud at Service	Oracle EE - 19c rel. 19.22	Oracle ExaCS Gen 2(X9M) Quarter Rack	OCPU: 188GB RAM: 1,2TB	20TB	5TB	BYOL

Tabella 318 – Database server CRESSAN

*Le risorse compute e storage sono condivise per tutti i database dipartimentali.

Per ulteriori dettagli sulla configurazione dei database, si rimanda al documento di progettazione EXACS.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

4.13.2.3 DNS

Nell'ambito della migrazione dei servizi applicativi SISaR, è prevista l'implementazione della funzionalità DNS sul Tenant centralizzato denominato CRESSAN. L'obiettivo è centralizzare la funzionalità per renderla fruibile anche nei Tenant periferici. Saranno quindi deployate sul Tenant Cressan del PSN 2 Virtual Machine VCRES-DNS1-PSN e VCRES-DNS2-PSN in sync bidirezionale ARES CRESSAN<->PSN CRESSAN tramite replica AD/Domain Controller. Tali VM avranno le seguenti caratteristiche:

- Sistema Operativo: Windows Server 2016 R2
- Funzionalità da abilitare: Domain controller, DNS, LDAP
- Configurazione zona unica: AD e Applicativa

Come riportato al paragrafo 4.12.2.1.1, è mandatoria l'adozione del sistema operativo Windows Server 2016 per le virtual machines VCRES-DNS1-PSN e VCRES-DNS2-PSN. Questa scelta è necessaria in quanto Windows Server 2016 rappresenta l'ultima versione del sistema operativo Microsoft compatibile con il functional level di Active Directory (AD) attualmente in uso nell'infrastruttura.

L'utilizzo di una versione più recente di Windows Server potrebbe richiedere un aggiornamento del Domain Functional Level (DFL) e del Forest Functional Level (FFL), operazione che potrebbe comportare impatti su servizi critici e sulla compatibilità con componenti legacy presenti nell'ambiente on-premise. Inoltre, Windows Server 2016 garantisce il pieno supporto per il Domain Name System (DNS) e il Domain Controller (DC), evitando potenziali problemi di interoperabilità con gli altri server e client già esistenti nella rete aziendale.

Pertanto, al fine di mantenere la stabilità e la compatibilità dell'ambiente Active Directory, senza introdurre modifiche strutturali che potrebbero compromettere l'integrazione con servizi dipendenti, si rende necessaria l'adozione di Windows Server 2016 per le macchine virtuali indicate.

Hostname	vCPU	RAM	Storage
VCRES-DNS1-PSN	4	12	70
VCRES-DNS2-PSN	4	12	70

Tabella 319 – DNS CRESSAN

4.13.2.4 Storage Condivisi

Non è presente nessuno share nei Tenant dipartimentali.

Tipologia di storage	Quantità allocato (TB)	Hostname (macchina se necessario)	Mount (se necessario)	Permessi (rw,r...)
Non presente	Non presente	Non presente	Non presente	Non presente

Tabella 320 – Storage condivisi CRESSAN

4.13.2.5 Networking

4.13.2.5.1 Schema di Rete

Per ragioni di leggibilità lo schema logico architetturale del networking relativo al servizio oggetto di trattazione nel presente documento è contenuto all'interno dell'Allegato 2 - Architettura di Networking Servizi Sisar.

4.13.2.5.2 Bilanciamento

Bilanciatori	IP Bilanciatore	VIP Bilanciatore	Hostname/FQDN/URL	Tipologia bilanciamento (LC, RR,...)	Persistenza sessione	Keepalive (TCP\URI,...)	Hostname da bilanciare (AS)	IP/Porta da bilanciare (AS)
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://hcsiots.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8281
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://formazioneAMCHR.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8194
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://ml-test.sisar.asl/diagnosiFunzionaleAreas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8180
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://mlts.sisar.asl/diagnosiFunzionaleAreas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8199

cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://prevenzionesevil.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 29080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://prevenzionetest.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 29090
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://portaleamiantotest.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8448
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://portaleamiantotest.sisar.asl/ras-sp	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8090
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://portalenpcwebtest.sisar.asl/ras-sp	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8090
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://hcsiot.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8281
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	/egrammata	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8183
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	/wsegrammata	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8183
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://attits.sisar.asl/ddd	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8183
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://rilascio.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://rilascio.sisar.asl/demon	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63: 8180
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://sidi-ts.sisar.asl/wdosidi	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8381
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://hcsiot.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8281
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://hcamchrt.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8071
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://demosan.sisar.asl/areas	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62: 8906

cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://sian-test.sisar.asl/SianWUI	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://sian-test.sisar.asl/SianWS	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://portalenpcwebtest.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san01-psn	10.77.2.62:8447
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://dipendente-ts.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63:28080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://spresal-ts.sisar.asl/Spresal	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63:8680
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://formazione-eliot.sisar.asl/WDOEliot	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	vcres-app-san02-psn	10.77.2.63:8086
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.156:443
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.156:8080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.156:8443
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.157:443
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.157:8080
cres-lbl1-psn	10.77.3.20	10.77.0.236 10.77.0.237 10.77.0.238	http://picassots.sisar.asl/	Adaptive RR/Failover	Con utilizzo di cookie	TCP/HTTP	N/A	10.3.67.157:8443

Tabella 321 – Bilanciamento CRESSAN

Tipo keepalive

Modalità di KeepAlive
TCP/HTTP

Tabella 322 – Tipo keepalive CRESSAN

Tipo persistenza sessione

Persistenza di Sessione
Persistenza basata su cookie

Tabella 323 – Tipo persistenza sessione CRESSAN

Tipologia balancing

Bilanciamento
Adaptive round robin o failover

Tabella 324 – Tipologia balancing CRESSAN

Tipo Domain Enable

Domain Enable
True

Tabella 325 – Tipo domain enable CRESSAN

Type

Type
Adaptive

Tabella 326 – Type CRESSAN

4.13.2.5.3 Reverse Proxy

Indirizzo IP RP	IP Virtual Host	Hostname Virtual Host	Where	What	Domain	Type	Enable domain	Real Address:port/URI Path	Note
N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A

Tabella 327 – Reverse proxy CRESSAN

4.13.2.5.4 Flussi e Accessibilità

4.13.2.5.4.1 Flussi interni

4.13.2.5.4.1.1 Flussi SIOAAP

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Contenuto flusso
Cressan centralizzato PSN	vcres-app- san01-psn	10.77.2.62	PICASSO	vip-picasso- test.sisar.asl/	10.3.61.23	TCP	443	From PSN to Picasso TEST

Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	AMC - TEST	formazioneamc hr.sisar.asl	10.3.66.40 (oggetto di migrazione OCI)	TCP	80	From PSN to AMC -TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	CUP - TEST	test- ticket.sardegna alute.it	82.85.18.173	TCP	443	From PSN to CUP WBS - test
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	CUP - TEST	formazionecup. sisar.asl	10.3.66.40	TCP	443	From PSN to CUP WBS - test
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	COT -TEST	cot- test.aressardeg na.it	93.39.83.54	TCP	443	From PSN to COT - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	VOUCHER- TEST	voucher- ts.sisar.asl	10.3.66.140 (oggetto di migrazione OCI)	TCP	443	From PSN to VOUCHER - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	DEMAPROT - TEST	demaprot- ts.sisar.asl	10.3.66.140 (oggetto di migrazione OCI)	TCP	443	From PSN to DEMAPROT - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	INAIL -TEST	spc.test.inail.it	93.147.161.63	TCP	443	From PSN to INAIL - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	CCER	*.cce.aressard egna.it	TBD (progetto in corso di realizzazione)	TCP	443	From PSN to CCER - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR VIEWER	medir.sardegna salute.it	195,130,213,208	TCP	443	From PSN to MEDIR
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR VIEWER	fse.sardegna alute.it	195,130,213,201	TCP	443	From PSN to MEDIR
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR GATEWAY	-	10.3.67.214	TCP	9508	From PSN to MEDIR
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	PICASSO	vip-picasso- test.sisar.asl/	10.3.61.23	TCP	443	From PSN to Picasso TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	AMC - TEST	formazioneamc hr.sisar.asl	10.3.66.40 (oggetto di migrazione OCI)	TCP	80	From PSN to AMC -TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	CUP - TEST	test- ticket.sardegna alute.it	82.85.18.173	TCP	443	From PSN to CUP WBS - test
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	CUP - TEST	formazionecup. sisar.asl	10.3.66.40	TCP	443	From PSN to CUP WBS - test
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	COT -TEST	cot- test.aressardeg na.it	93.39.83.54	TCP	443	From PSN to COT - TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	VOUCHER- TEST	voucher- ts.sisar.asl	10.3.66.140 (oggetto di migrazione OCI)	TCP	443	From PSN to VOUCHER - TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	DEMAPROT - TEST	demaprot- ts.sisar.asl	10.3.66.140 (oggetto di migrazione OCI)	TCP	443	From PSN to DEMAPROT - TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	INAIL -TEST	spc.test.inail.it	93.147.161.63	TCP	443	From PSN to INAIL - TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	CCER	*.cce.aressard egna.it	TBD (progetto in corso di realizzazione)	TCP	443	From PSN to CCER - TEST
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR VIEWER	medir.sardegna salute.it	195,130,213,208	TCP	443	From PSN to MEDIR

Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR VIEWER	fse.sardegna.ute.it	195,130,213,201	TCP	443	From PSN to MEDIR
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	MEDIR GATEWAY	-	10.3.67.214	TCP	9508	From PSN to MEDIR

Tabella 328 - Flussi SIOAAP CRESSAN

4.13.2.5.4.1.2 Flussi SIOAAP - Connessione a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Contenuto flusso
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	DB - TEST CUP	cres-dbtest1.sisar.asl	10.3.67.155	TCP	1521	From PSN to DB CUP - TEST
Cressan centralizzato PSN	vcres-app-san02-psn	10.77.2.63	DB - TEST CUP	cres-dbtest1.sisar.asl	10.3.67.155	TCP	1521	From PSN to DB CUP - TEST

Tabella 329 - Flussi SIOAAP CRESSAN - Connessioni a DB

4.13.2.5.4.2 Flussi esterni

4.13.2.5.4.2.1 Flussi PICASSO

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Contenuto flusso
Picasso	worker-node-01	10.3.61.50	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-02	10.3.61.51	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-03	10.3.61.52	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-04	10.3.61.53	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-05	10.3.61.54	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-06	10.3.61.55	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-07	10.3.61.56	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Picasso	worker-node-08	10.3.61.57	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN

Picasso	worker-node-09	10.3.61.58	Cressan centralizzato PSN	cres-vip1 cres-vip2 cres-vip3	10.77.0.236 10.77.0.237 10.77.0.238	TCP	80	From Picasso to PSN
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.62	Picasso	https://vip-picasso-test.sisar.asl/	N/A	TCP	443	From PSN to Picasso
Cressan centralizzato PSN	vcres-app-san01-psn	10.77.2.63	Picasso	https://vip-picasso-test.sisar.asl/	N/A	TCP	443	From PSN to Picasso

Tabella 330 - Flussi PICASSO CRESSAN

4.13.2.5.4.2.2 Flussi PICASSO – Connessioni a DB

Sistema source	Hostname \ DNS source	IP source	Sistema destination	Hostname \ DNS destination	IP destination	Protocollo \ tecnologia	Porta	Contenuto flusso
Picasso	worker-node-01	10.3.61.50	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-02	10.3.61.51	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-03	10.3.61.52	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-04	10.3.61.53	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-05	10.3.61.54	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-06	10.3.61.55	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-07	10.3.61.56	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-08	10.3.61.57	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS
Picasso	worker-node-09	10.3.61.58	Oracle ExaCS	TBD	Listener EXACS	TCP	1521	From Picasso to PSN EXACS

Tabella 331 - Flussi PICASSO - Connessione a DB CRESSAN

4.13.2.5.4.2.3 Flussi SPAGIC

I flussi SPAGIC attualmente in uso nell'infrastruttura on-premise non sono oggetto di censimento, poiché è stato pianificato il loro imminente phase-out.

4.13.2.6 Sicurezza

4.13.2.6.1 Autenticazione

I servizi Sisar ad uso interno hanno un'autenticazione con utente/password nel database dipartimentale.

4.13.2.6.2 Certificati SSL

Per il solo servizio PUA Comuni viene utilizzato un certificato di tipo wildcard fornito dall'Amministrazione (*.sardegnaasalute.it) e si prevede che lo stesso verrà installato da Leonardo sul WAF dello IaaS target. A tale

proposito l'Amministrazione dovrà autorizzare Leonardo all'utilizzo di tale certificato e relativa chiave sui propri dispositivi.

4.13.2.6.3 Micro-segmentazione

In un'ottica di rafforzamento della sicurezza, il tenant CRESSAN, concepito come contenitore di più applicazioni, adotterà un modello di microsegmentazione. La soluzione pianificata utilizza i VM tags per organizzare le macchine virtuali in dynamic groups.

Questa configurazione sarà progettata per garantire una gestione scalabile e precisa delle comunicazioni e delle politiche di sicurezza, articolata come segue.

Raggruppamento per Servizi Applicativi:

- Le macchine virtuali verranno classificate in dynamic groups, ognuno dei quali corrisponderà a un servizio applicativo specifico. Tale organizzazione permetterà di ottenere un isolamento logico tra i servizi, migliorando la chiarezza e l'efficienza della gestione.

Politiche di Comunicazione:

- Stesso gruppo e layer applicativo: Le VM appartenenti allo stesso dynamic group e operanti nello stesso layer applicativo (ad esempio, il layer dati) potranno comunicare liberamente, rispettando le configurazioni di sicurezza già impostate sui sistemi operativi; (Figura 14)
- Stesso gruppo ma layer applicativo differente: Le comunicazioni tra VM appartenenti allo stesso dynamic group, ma situate in layer applicativi diversi, saranno gestite tramite NGFW, con l'applicazione di policy configurate ad hoc; (Figura 15)
- Gruppi diversi: Non sarà consentita alcuna comunicazione tra VM appartenenti a dynamic groups distinti, né all'interno dello stesso layer applicativo, né tra layer diversi, assicurando un isolamento completo.

Questa configurazione permetterà di ottenere un isolamento rigoroso tra i diversi progetti e servizi, migliorando al contempo l'efficienza operativa nella gestione delle politiche di sicurezza. La centralizzazione delle regole, basata sui dynamic groups, semplificherà notevolmente le attività di configurazione e manutenzione delle policy.

Nel caso specifico di CRESSAN nella tabella 315 sono riportati i VM Tags e Dynamic Group individuati per segregare il traffico con le altre applicazioni presenti nel tenant, in dettaglio Rischio Clinico e Assistenza Residenziale e Semi Residenziale.

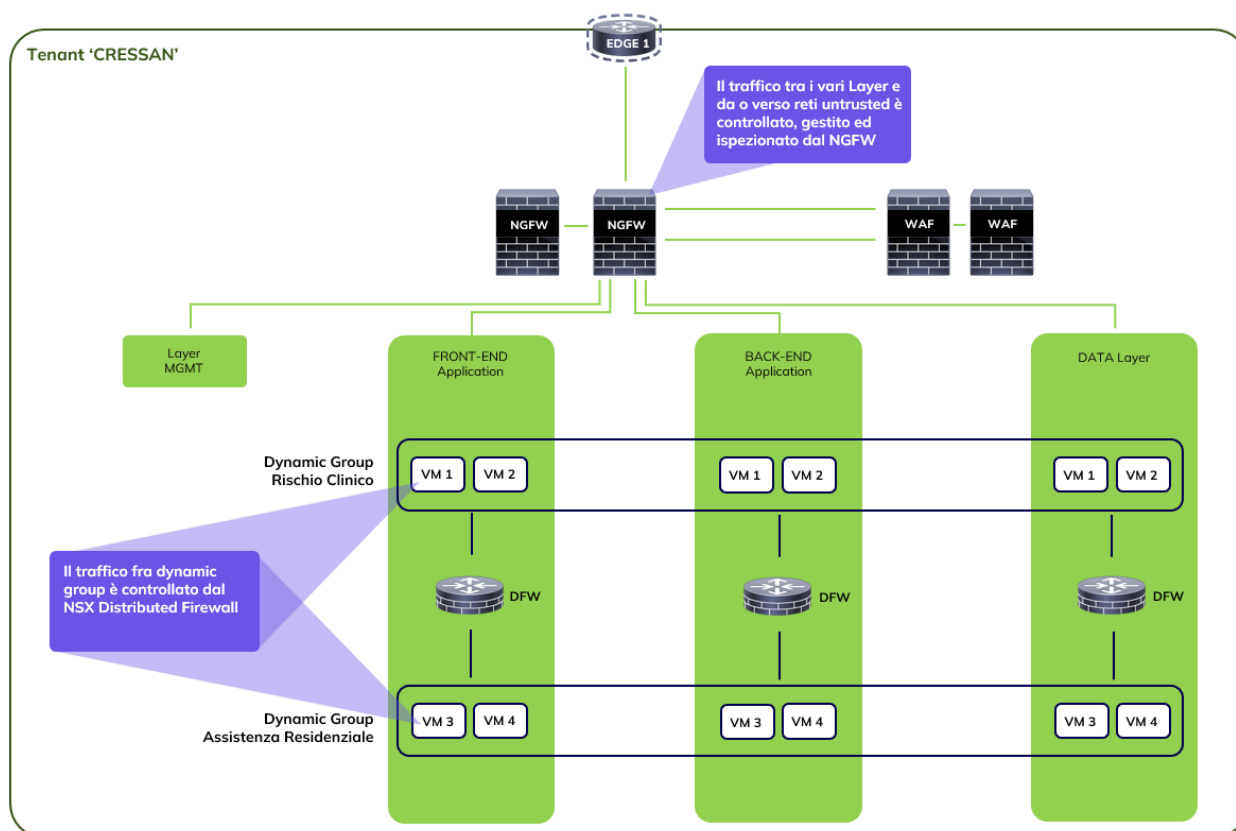


Figura 14 - Soluzione di microsegmentazione Cressan - Intra Layer

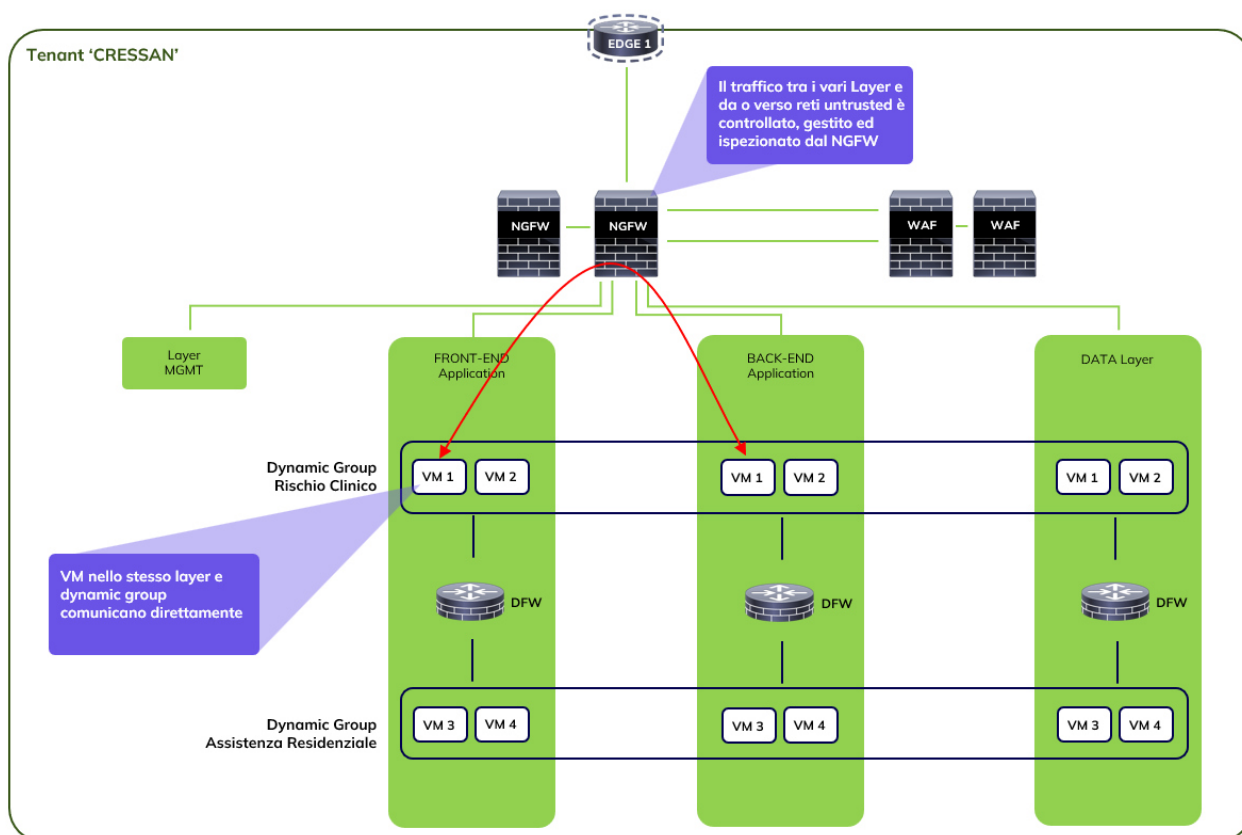


Figura 15 - Soluzione di microsegmentazione Cressan - Extra Layer

4.13.2.6.4 Regole Firewall

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.0.0/24	10.77.2.60		TCP-UDP UDP TCP TCP-UDP TCP-UDP UDP TCP TCP-UDP	53 123 25 445 88 389 636 464	Subnet FE to DNS/DC/AD (VCRES- DNS1-PSN)

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.0.0/24	10.77.2.61		TCP-UDP UDP TCP TCP-UDP TCP-UDP UDP TCP TCP-UDP	53 123 25 445 88 389 636 464	Subnet FE to DNS/DC/AD (VCRES- DNS2-PSN)
10.77.0.0/24	10.77.2.62		TCP	8281 8180 29080 8448 8090 8183 8080 8381 8071 8906 8447 28080 8680	Subnet FE to vcres- app-san01-psn
10.77.0.0/24	10.77.2.63		TCP	8281 8180 29080 8448 8090 8183 8080 8381 8071 8906 8447 28080 8680	Subnet FE to vcres- app-san02-psn
10.77.2.62	Listener EXACS		TCP	1521	vcres-app-san01-psn to ExaCS
10.77.2.63	Listener EXACS		TCP	1521	vcres-app-san02-psn to ExaCS

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.2.60	10.3.67.51		UDP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP	123 135 464 49152-65535 389 636 3268 3269 53 49152-65535 88 445 49152-65535	VCRES-DNS1-PSN to vcred-infra1
10.77.2.60	10.3.67.52		UDP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP	123 135 464 49152-65535 389 636 3268 3269 53 49152-65535 88 445 49152-65535	VCRES-DNS1-PSN to vcred-infra2
10.77.2.61	10.3.67.51		UDP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP	123 135 464 49152-65535 389 636 3268 3269 53 49152-65535 88 445 49152-65535	VCRES-DNS1-PSN to vcred-infra1

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.2.61	10.3.67.52		UDP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP TCP/UDP TCP TCP/UDP TCP TCP TCP	123 135 464 49152-65535 389 636 3268 3269 53 49152-65535 88 445 49152-65535	VCRES-DNS1-PSN to vcres-infra2
10.38.0.120	10.77.2.62		TCP	8183	to vcres-app-san01- psn
10.39.254.17	10.77.2.62		TCP	8447	to vcres-app-san01- psn
10.79.2.32/28	10.77.2.63		TCP	8183	to vcres-app-san02- psn
10.77.2.62	10.3.61.23		TCP	443	From PSN to Picasso TEST
10.77.2.62	10.3.66.40 (oggetto di migrazione OCI)		TCP	80	From PSN to AMC - TEST
10.77.2.62	82.85.18.173		TCP	443	From PSN to CUP WBS - test
10.77.2.62	10.3.66.40		TCP	443	From PSN to CUP WBS - test
10.77.2.62	93.39.83.54		TCP	443	From PSN to COT - TEST
10.77.2.62	10.3.66.140 (oggetto di migrazione OCI)		TCP	443	From PSN to VOUCHER - TEST
10.77.2.62	10.3.66.140 (oggetto di migrazione OCI)		TCP	443	From PSN to DEMAPROT - TEST
10.77.2.62	93.147.161.63		TCP	443	From PSN to INAIL - TEST
10.77.2.62	TBD (progetto in corso di realizzazione)		TCP	443	From PSN to CCER - TEST
10.77.2.62	195.130.213.208		TCP	443	From PSN to MEDIR
10.77.2.62	195.130.213.201		TCP	443	From PSN to MEDIR

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.77.2.62	10.3.67.214		TCP	9508	From PSN to MEDIR
10.77.2.63	10.3.61.23		TCP	443	From PSN to Picasso TEST
10.77.2.63	10.3.66.40 (oggetto di migrazione OCI)		TCP	80	From PSN to AMC - TEST
10.77.2.63	82.85.18.173		TCP	443	From PSN to CUP WBS - test
10.77.2.63	10.3.66.40		TCP	443	From PSN to CUP WBS - test
10.77.2.63	93.39.83.54		TCP	443	From PSN to COT - TEST
10.77.2.63	10.3.66.140 (oggetto di migrazione OCI)		TCP	443	From PSN to VOUCHER - TEST
10.77.2.63	10.3.66.140 (oggetto di migrazione OCI)		TCP	443	From PSN to DEMAPROT - TEST
10.77.2.63	93.147.161.63		TCP	443	From PSN to INAIL - TEST
10.77.2.63	TBD (progetto in corso di realizzazione)		TCP	443	From PSN to CCER - TEST
10.77.2.62	195.130.213.208		TCP	443	From PSN to MEDIR
10.77.2.62	195.130.213.201		TCP	443	From PSN to MEDIR
10.77.2.62	10.3.67.214		TCP	9508	From PSN to MEDIR
10.77.2.62	10.3.67.155		TCP	1521	From PSN to DB CUP - TEST
10.77.2.63	10.3.67.155		TCP	1521	From PSN to DB CUP - TEST
10.3.61.50	10.77.0.236 10.77.0.237 10.77.0.238		TCP	80	From Picasso to PSN
10.3.61.51	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.236	From Picasso to PSN
10.3.61.52	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.237	From Picasso to PSN

Rete / IP Sorgente	Rete / IP Destinazione	Protocollo	TCP / UDP	Porte	Note
10.3.61.53	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.238	From Picasso to PSN
10.3.61.54	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.236	From Picasso to PSN
10.3.61.55	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.237	From Picasso to PSN
10.3.61.56	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.238	From Picasso to PSN
10.3.61.57	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.236	From Picasso to PSN
10.3.61.58	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.237	From Picasso to PSN
10.77.2.62	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.238	From Picasso to PSN
10.77.2.63	10.77.0.236 10.77.0.237 10.77.0.238		TCP	10.77.0.236	From Picasso to PSN
10.3.61.50	Listener EXACS		TCP	1521	From Picasso to PSN EXACS
10.3.61.51	Listener EXACS		TCP	1521	From Picasso to PSN EXACS
10.3.61.52	Listener EXACS		TCP	1521	From Picasso to PSN EXACS
10.3.61.53	Listener EXACS		TCP	1521	From Picasso to PSN EXACS
10.3.61.54	Listener EXACS		TCP	1521	From Picasso to PSN EXACS
10.3.61.55	Listener EXACS		TCP	1521	From Picasso to PSN EXACS

Tabella 332 – Regole firewall CRESSAN

4.13.2.7 Licenze

La licenza per il database Oracle Exadata Cloud Service sarà in modalità BYOL (Bring Your Own License).

4.13.2.8 Policy di Backup

Dal punto di vista infrastrutturale, oltre alle risorse computazionali (vCPU, RAM, Disco, SO, ...), è stato previsto anche il servizio Data Protection Backup di CommVault (v 11.28) che consente, tramite un'unica console centralizzata, la gestione in piena autonomia da parte dell'Amministrazione della protezione dei dati sia on-premise (Datacenter PSN) che presso i vari cloud service provider di una infrastruttura IT di tipo multi-cloud. Il servizio consente l'esecuzione di backup e restore di contesti cliente in modo efficace e sicuro sia on-premise che su cloud provider. I contesti da proteggere possono essere di varia tipologia (file, virtual machine, tutti i principali database, es. SAP, Exchange, SQL, DB2, PostgreSQL, GPFS, MongoDB, Hadoop, Kubernetes, etc.). I dati di backup relativi ai tredici tenant di ARES Sardegna saranno storicizzati su un unico repository. All'interno di questo repository, gli elementi oggetto di backup associati al servizio di Emergenza Sanitaria Territoriale 118 saranno raggruppati logicamente in un unico gruppo. In sostanza, viene implementata una segmentazione a livello di servizio applicativo da migrare su cloud PSN.

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

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

Il servizio Data Protection Backup è un servizio di tipo «self-managed», questo significa che l'Amministrazione ha la responsabilità della scelta delle policy di backup, del restore e di tutte le configurazioni disponibili sulla console centralizzata messa a disposizione. Il PSN è responsabile del corretto funzionamento di tutto ciò che sta al di sotto della console. Per i dettagli tecnici sull'utilizzo e le funzionalità della console, consultare la guida reperibile dalla console del servizio selezionando la voce "Web Console" dal menu di sinistra.

Il servizio Data Protection Backup contrattualizzato da ARES Sardegna dispone anche della funzionalità aggiuntiva della Golden Copy.

Tale funzionalità è completamente gestita in aggiunta al servizio core: essa effettua la verifica e convalida dell'integrità dei dati durante le attività di backup e di esecuzione della Golden Copy. Questa modalità, insieme alle ulteriori procedure di sicurezza per l'accesso ai sistemi e alle applicazioni, garantisce la conservazione dei backup in un formato non cancellabile e inalterabile (WORM: Write Once, Read Many) e assicura che le attività di gestione operativa di routine (es. svecchiamento delle retention scadute) siano sempre sotto la competenza e il controllo di autorità di supervisione che non possono essere by-passate.

Ulteriori meccanismi di protezione dei dati impediscono la modifica o l'eliminazione dei file per un periodo di conservazione definito dalle policy utente o del sistema di backup (golden copy definita come WORM copy che non permette a nessuno, lato piattaforma di backup di cancellare i dati prima della loro scadenza).

Inoltre, sui sistemi sorgenti, in aggiunta ai tradizionali sistemi di protezione antivirus/antimalware, è possibile attivare meccanismi di identificazione di eventuali ransomware in maniera proattiva: qualsiasi attività sospetta sul file system dei sistemi da proteggere viene intercettata e segnalata alla console di gestione attraverso l'invio di allarmi che opportunamente gestiti consentono di condizionare e inibire la creazione della golden copy. Tale funzionalità aggiuntiva di controllo ransomware alla fonte, da applicarsi alle macchine in esercizio e che richiederebbe degli specifici strumenti di scansione, non è prevista da progetto in quanto è stato ritenuto che gli strumenti resi disponibili (Vulnerability Assessment, Research & Exploitation, Dynamic Application Security Testing, Supporto Device Management Protezione Perimetrale NGFW e WAF, etc.) siano sufficienti a garantire la protezione dell'infrastruttura.

Le copie di backup potranno essere protette da ulteriori configurazioni, a livello di sottosistema storage, da eventuali attacchi di tipo ransomware non permettendo ad alcun processo esterno di modificare i dati salvati nei backup: solo per le copie su cui non sarà stata segnalata alcuna anomalia di tipo ransomware, si potrà procedere all'archiviazione della golden copy in un ambiente protetto e in sola lettura.

Le principali caratteristiche del servizio sono:

Analisi automatizzata del backup per certificarne l'assenza di vulnerabilità (incluse attività sospette di ransomware):

- Protezione su storage distinto di backup, privo di ogni accesso fisico e logico;
- Replica in Region diverse e su canale cifrato;
- Le policy della Golden Copy saranno di default analoghe a quelle impostate dal cliente per il servizio Data Protection Backup;
- Tale servizio potrà essere applicato a un sottoinsieme dei file per cui è stato richiesto dal cliente il servizio Data Protection Backup.

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

- Air Gap:
 - Ambiente di replica isolato accessibile solo ai processi di backup. L'accesso fisico alle risorse isolate è protetto e fortemente controllato;
 - Tutte le comunicazioni di rete in entrata (sul target di replica) sono bloccate al di fuori della finestra temporale di replica;
 - Replica dei dati con tunnel sicuro;
 - Tutto l'accesso ai dati isolati è bloccato. È consentita solo l'inizializzazione di connessioni in uscita dai dati isolati ai dati di origine per la replica. Tale modalità è gestita dalla tecnologia di riferimento (Commvault) attraverso opportune configurazioni (Topology network and tunnel configuration per garantire ambiente AIR-GAP).
- WORM Protection:

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

Nell'ambito della migrazione dei servizi dipartimentali SiSar, il servizio di Data Protection Backup di CommVault verrà configurato durante la fase di predisposizione dell'infrastruttura per eseguire il backup di tutte le VM e di tutti i sistemi DBMS tramite l'installazione/attivazione di un agent su ogni sistema. L'obiettivo è quello di mantenere la coerenza dei dati durante il backup attraverso l'abilitazione dell'opzione della quiescenza. Su tutti i backup sarà prevista l'applicazione della funzionalità di Golden Copy.

In accordo con l'Amministrazione, in fase pre-migrazione, verranno condotti dei test di restore manuali mirati sulle componenti critiche dell'architettura dei servizi dipartimentali SiSar. Lo scopo di questi test è duplice: da un lato, verificare il corretto funzionamento del meccanismo di backup e restore; dall'altro, supportare l'Amministrazione nella definizione di procedure operative da seguire in caso di necessità di ripristino, ad esempio per risolvere problematiche che potrebbero verificarsi a seguito della migrazione del servizio su PSN.

Per quanto riguarda la localizzazione dei backup, il servizio Data Protection Backup per ARES Sardegna è istanziato nella Region Sud. Ciò significa che le copie di backup vengono replicate nei Data Center di Acilia e Pomezia. Invece, le copie relative alla Golden Copy vengono conservate nella Regione Nord (Rozzano-Santo Stefano Ticino).

Gli SLA associati al servizio Data Protection Backup con Golden Copy sono normati nell'allegato H - Indicatori di Qualità, al capitolo 2 ID: IQ010: Disponibilità del servizio di IaaS, PaaS, BaaS, CaaS. Di seguito si riportano gli elementi salienti:

- Disponibilità del servizio, soglia minima $\geq 99,95\%$;
- Rispetto RTO, valore target 30 minuti;
- Rispetto RPO, valore target 15 secondi.

La tabella seguente dettaglia le policy di backup proposte.

Hostname	IP	Oggetto backup (es: copia VM, contenuto database, configurazioni, etc)	Modalità \ strumento di backup (es: RMAN, immagine)	Frequenza (n volte al giorno / settimana / mese)	Retention (gg)
aouca-app-san1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
aouca-app-san2-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
cres-lbl1-psn		Snapshot VM	Data Protection Backup & Golden Copy	1 volta al giorno	30 gg
Exadata		Contenuto Database	Data Protection Backup & Golden Copy	<ul style="list-style-type: none"> • Backup Full 1 volta a settimana; • Backup incrementale 1 volta al giorno; • Backup Archivelog ogni 2 ore. 	30 gg

Tabella 333 – Policy di backup CRESSAN

4.13.2.9 Policy di DR

Con riferimento a quanto già specificato al capitolo “5.2.4 Data Protection e Disaster Recovery” del Progetto del Piano dei Fabbisogni (ID 2023-0000003990570925-PPdF-P1R1), in linea con quanto attualmente in campo, l’Amministrazione ha espresso la volontà di non utilizzare servizi di Disaster Recovery in questo progetto di migrazione a PSN, riservandosi di effettuare una analisi più approfondita del fabbisogno in una fase successiva.

5 STRATEGIA DI MIGRAZIONE

L'architettura del parco applicativo SISAR si basa su un modello monolitico, in cui tutti i servizi e le funzionalità applicative sono strettamente integrati e risiedono all'interno della stessa macchina virtuale (VM). I servizi utilizzano un unico database centrale e accedono agli stessi schema.

La migrazione Lift & Shift dall'ambiente on-premise al cloud viene realizzata senza modificare la struttura del software o la sua logica di funzionamento. Questo significa che l'organizzazione e la disposizione dei servizi all'interno della VM rimangono inalterate rispetto alla configurazione originale. In un modello Lift & Shift, infatti, l'obiettivo principale è replicare fedelmente l'ambiente esistente in una nuova infrastruttura, garantendo continuità operativa senza la necessità di refactoring o riprogettazione dell'applicazione.

Di conseguenza, se più servizi sono installati sulla stessa macchina fisica o virtuale nell'ambiente on-premise, questa configurazione viene mantenuta anche dopo la migrazione. Ogni servizio continua a operare all'interno della stessa VM come avveniva in precedenza, interagendo con gli altri componenti tramite le stesse chiamate e dipendenze esistenti. Anche l'accesso al database centrale rimane invariato, preservando le stesse logiche di gestione dei dati e la stessa configurazione degli schema.

Di seguito sono riportate le architetture as-is ad alto livello dei sistemi dipartimentali e delle aziende ospedaliere universitarie, con l'elenco delle applicazioni esposte:

Dipartimentale

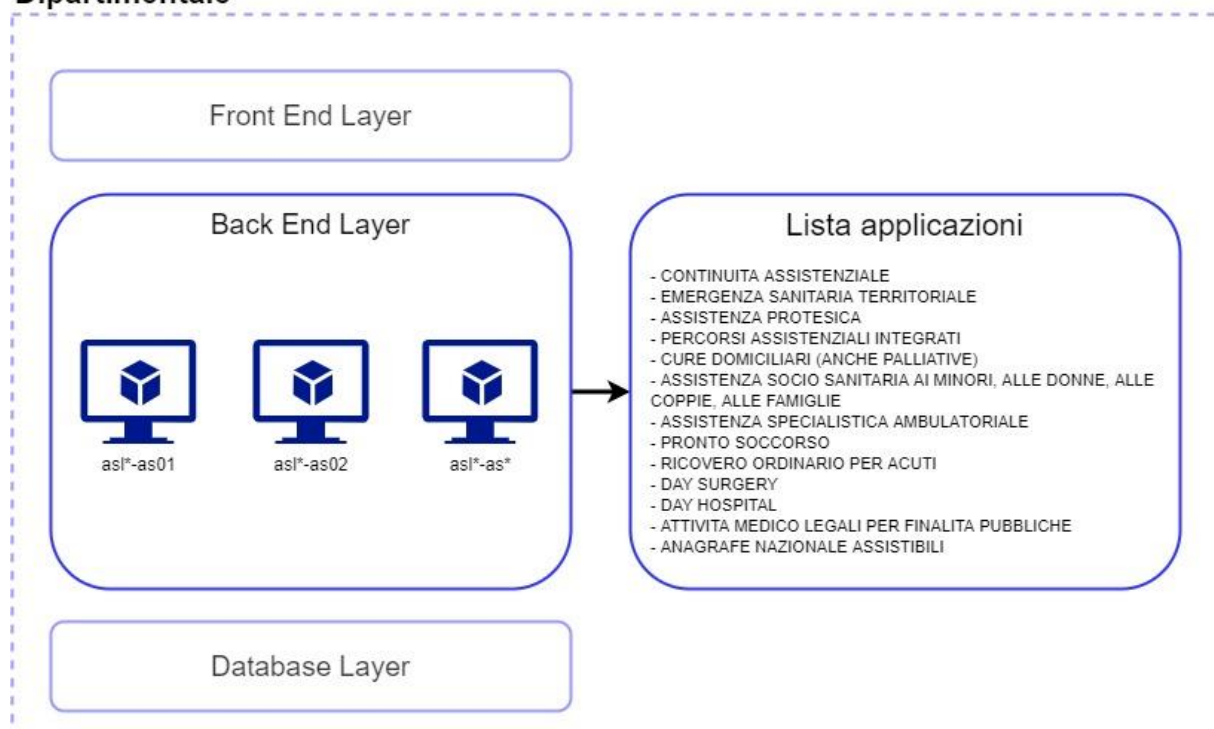


Figura 16 - Applicazioni esposte dai dipartimentali ambiente as-is.

AOU - Azienda Ospedaliera Universitaria

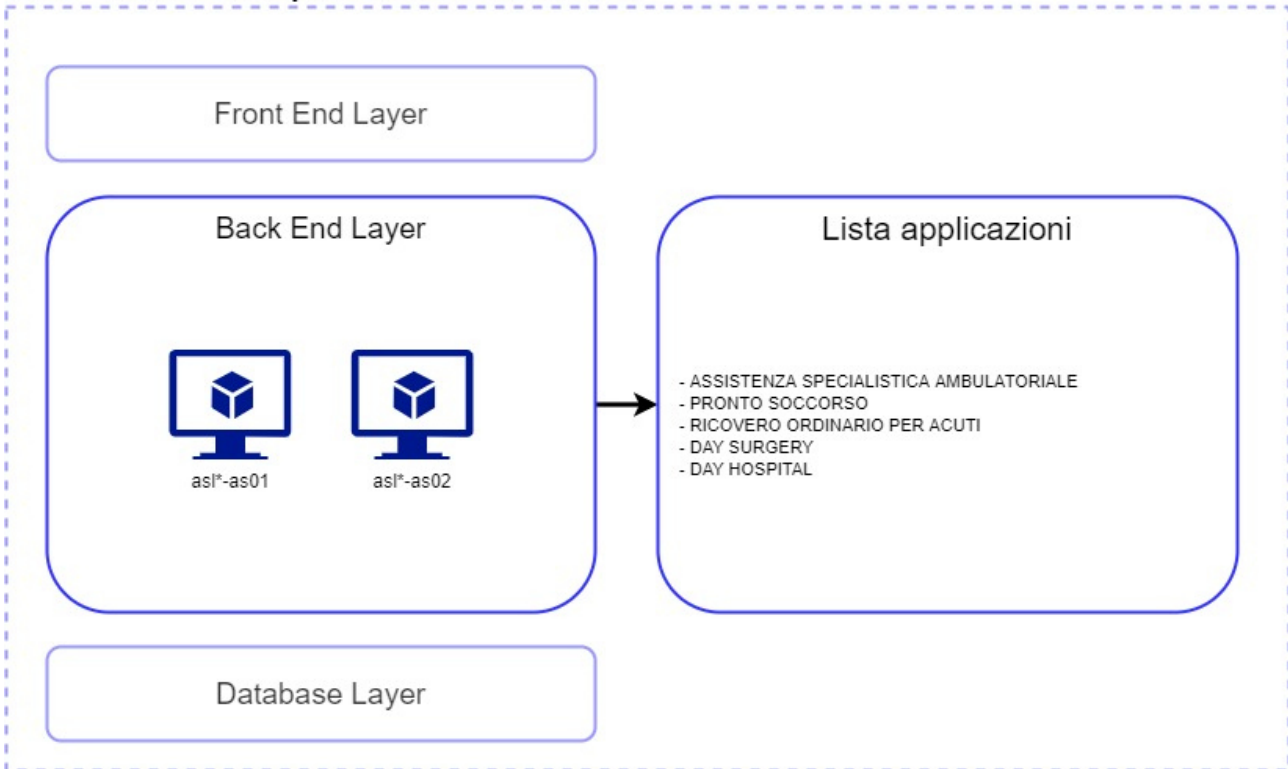


Figura 17 - Applicazioni esposte dalle AOU ambiente as-is.

Questa configurazione comporta numerose limitazioni tecniche nella strategia di migrazione basata sul servizio, tra cui:

- **Migrazione Database:**

- La migrazione parziale del database non è possibile a causa dell'assenza di segregazione dei dati a livello di servizio. La struttura del database è consolidata su un'unica VM e gli schema non costituiscono un elemento caratterizzante ed esclusivo di ogni servizio.
- La separazione degli schema potrebbe causare problematiche di latenza e revisione del codice applicativo sorgente.
- La necessità di migrare contemporaneamente tutti i database dipartimentali costituisce un ostacolo significativo, particolarmente nel caso di database di ampie dimensioni.

- **Migrazione VM:**

- La strategia basata su servizio richiede la migrazione simultanea di tutte le VM dipartimentali relative al servizio in scope;
- Necessità di implementare regole di bilanciamento del carico cross-datacenter;
- Aumenta la complessità della gestione infrastrutturale, aumentando il rischio di disservizi durante la transizione;

- Aumenta la complessità della migrazione in quanto richiede un allineamento dell'applicativo con strumenti non standard.
 - Rework delle configurazioni lato applicazione per inibire i servizi oggetto di migrazione sull'ambiente as-is.
 - Rework delle configurazioni lato applicazione per inibire i servizi non oggetto di migrazione sull'ambiente to-be.
- **Ambiente VMware di transito:**
 - La migrazione simultanea di tutte le VM richiede un dimensionamento molto più oneroso per l'ambiente di transito. Con la strategia di migrazione basata sul servizio, l'ambiente dovrà essere in grado di ospitare tutte le VM contemporaneamente, a differenza della strategia di migrazione basata sui tenant, dove l'ambiente verrà dimensionato sul il massimo dimensionamento tra tutti i dipartimenti.
 - **Incompatibilità con il Lift and Shift (L&S):**
 - La strategia non è compatibile con l'approccio lift and shift (L&S), che prevede lo spostamento diretto delle applicazioni senza apportare nessuna modifica.
 - **Impatto Globale:**
 - In caso di problemi durante la migrazione, si potrebbe verificare un impatto globale su tutti i servizi di tutti i dipartimenti.

In conclusione, la migrazione sul PSN basata sul servizio del parco applicativo SISAR presenta numerosi ostacoli e rischi, pertanto per ridurre l'impatto e avere una gestione più controllata della migrazione è consigliabile utilizzare la strategia per "tenant".

5.1 PIANIFICAZIONE DELLA MIGRAZIONE

Il Gantt mostrerà la pianificazione della migrazione in tutte le sue fasi, evidenziando le attività principali, i tempi di realizzazione e le eventuali dipendenze tra le diverse fasi. Questo strumento permetterà di visualizzare chiaramente le tempistiche e i progressi, consentendo una gestione efficiente e un monitoraggio continuo del progetto. Il Gantt è in allegato al seguente documento.

5.2 PREDISPOSIZIONE AMBIENTI TO-BE

5.2.1 Configurazione Ambiente

Prima di procedere alla migrazione dei workload sarà necessario configurare l'ambiente messo a disposizione dal PSN. Le macro-attività indicate nella successiva tabella saranno eseguite sul singolo Tenant tramite accesso alla console di gestione.

A titolo di esempio viene riportato il Tenant dedicato all'ASL1:

Task	Ambiente	Owner	Vincoli
Predisposizione di Rete	ASL1	LDO	
Predisposizione dispositivi di sicurezza (WAF, NGF, Natting)	ASL1	LDO	
Predisposizione/Configurazione NSG	ASL1	LDO	
Predisposizione/Configurazione VPN	ASL1	LDO	
Predisposizione/Configurazione vCDA	ASL1	PSN/ACN	Connettività MPLS/Internet con tenant di transito
Peering vCDA	ASL1	ACN	URL, USER, PWD vCDA PSN
Configurazione replica vCDA	ASL1	ACN	Accesso ambiente target PSN
Migrazione Virtual machine	ASL1	ACN	Accesso ambiente target PSN
Check post migrazione (accesso RDP, SSH e verifica risorse)	ASL1	ACN	Accesso ambiente target PSN
Riconfigurazione VM (DNS, Database etc.)	ASL1	ACN	Accesso ambiente target PSN

Tabella 334 – Configurazione ambiente To-Be

5.2.2 Migrazione Workload

Di seguito viene rappresentata la strategia di migrazione delle virtual machine dall'ambiente On-premise verso il PSN.

Per eseguire tale attività è necessario avere a disposizione le seguenti componenti:

- Vmware vCenter Converter On-premise;
- Ambiente di transito con hypervisor Vmware, il dimensionamento di tale sito è stato calcolato sulla base delle risorse MAX allocate per tutti i tenant in scope di migrazione;

	CPU TOTALE (vCPU)	RAM Totale (GB)	Storage Totale (GB)
Size Vmware Transito	38	168	880

Tabella 335 - Dimensionamento sito di transito

- Connettività tra DC On-premise e sito di transito su CRESSAN;
- Connettività tra sito di transito CRESSAN e ambiente target messo a disposizione dal PSN;
- Peering vCDA tra sito di transito CRESSAN e ambiente target messo a disposizione dal PSN.

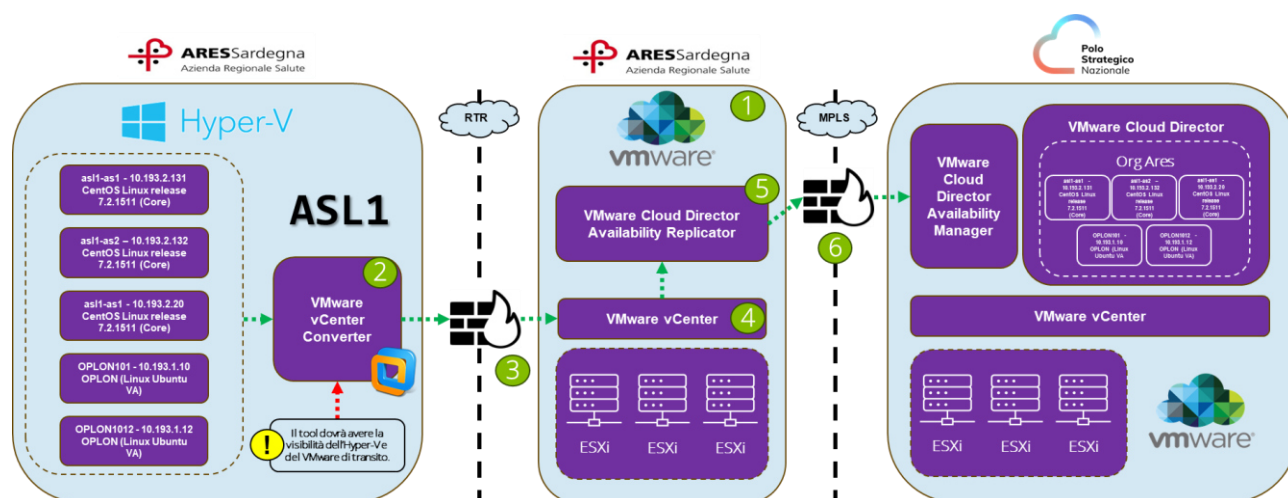


Figura 18 - Strategia di migrazione virtual machine

ID	Task	Ambiente	Durata (*)	Owner	Vincoli
1	Distribuire e configurare il sito VMware di Transito.	On-prem transit	TBD	SardegnaIT	Accesso al sito di transito
2	Distribuire vCenter Converter Standalone e i suoi componenti nel sito di origine	On-prem	TBD	SardegnaIT	Necessario che il tool abbia visibilità con l'Hyper-v e VMware di transito
3	Convertire con Converter una macchina virtuale nel sito di Transito.	On-prem to On-prem transit	TBD	SardegnaIT	Connettività tra DC On-premise e sito di transito;
4	Verificare che tutte le proprietà (tipo di GuestOS, versione, controller SCSI, ecc.) siano popolate correttamente attraverso l'interfaccia utente di vSphere.	On-prem transit	TBD	SardegnaIT	Accesso al sito di transito
5	Installazione e configurazione VMware Cloud Director Availability sul sito di transito.	On-prem transit	TBD	SardegnaIT	Accesso al sito di transito
6	Configurare la migrazione utilizzando VMware Cloud Director Availability	PSN	TBD	ACN	- Connettività tra sito di transito e ambiente target messo a disposizione dal PSN. - Peering vCDA
7	Avvio migrazione	On-prem transit to PSN	TBD	ACN	N/A

Tabella 336 - Task strategia di migrazione virtual machine

* Le stime dei tempi per ciascun task saranno calcolate una volta che tutte le componenti saranno disponibili per eseguire test case reali.

5.3 MIGRAZIONE DATI

5.3.1 Modalità di Migrazione – Golden Gate

Nel seguente paragrafo viene illustrata la procedura di migrazione tramite GoldenGate relativo ai DB presenti in ciascun dipartimentale, con i relativi step di esecuzione.

Un requisito fondamentale della soluzione proposta è la visibilità, in termini di connettività, da parte del componente GoldenGate Manager, sia del database sorgente attraverso le reti RTR/MPLS, sia del database di destinazione. La strategia di replica dei dati si fonda sulla capacità di Oracle GoldenGate di catturare e trasferire in tempo reale le modifiche dai database sorgente a quelli di destinazione, assicurando una sincronizzazione continua e accurata tramite i processi di Extract e Replicat.

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

La strategia prevedere i seguenti step:

Pre-cutover:

ID	Task	Ambiente	Durata (*)	Owner	Vincoli
1	start cattura delle modifiche sul DB sorgente con GG	PSN	NO DOWNTIME		
2	backup full + archivelog del DB sorgente (RMAN)	On-premise			
3	restore e recover iniziali ad un SCN XXX sul DB target (RMAN)	PSN			
4	apertura DB target e conversione in PDB	PSN			
5	start replica delle modifiche catturate con GG, dall'SCN XXX+1 in poi sul DB target	PSN			

Tabella 337 - Task Pre-cutover - Golden Gate

Cutover:

ID	Task	Ambiente	Durata (*)	Owner	Vincoli
1	stop gli applicativi	On-premise	50 min		
2	stop e inversione replica	On-premise /PSN			
3	start applicativi	PSN			

Tabella 338 - Task Cutover - Golden Gate

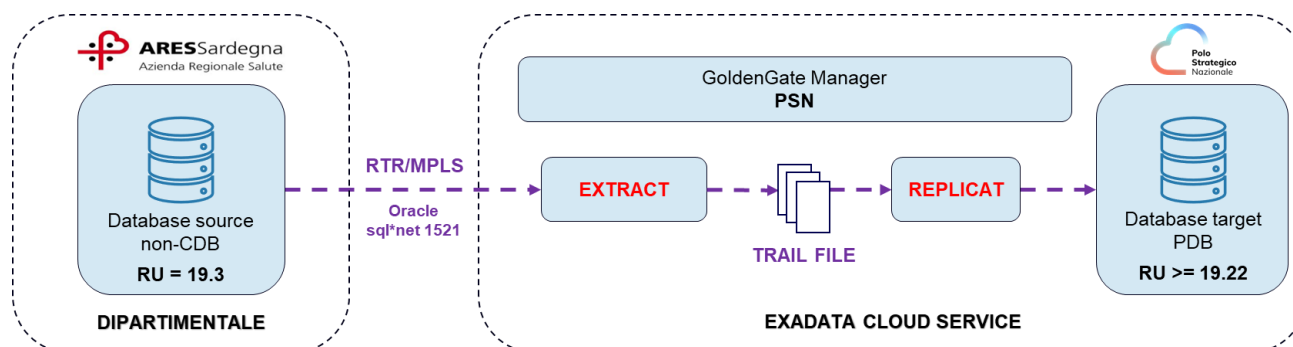


Figura 19 - Strategia di Migrazione - Golden Gate

Di seguito un approfondimento dei punti 2 e 3 menzionati nella fase di pre-cutover in quanto per eseguire il primo import dei dati si utilizzerà lo strumento RMAN. Terminato questo processo si potrà attivare GG che si occuperà di sincronizzare il DB in tempo reale.

Pre-cutover

ID	Task	Ambiente	Durata (*)	Owner	Vincoli
1	Backup incrementale a livello 0 (o full backup, includendo control file) del DB AS-IS + archivelog del DB AS-IS tramite recovery manager (RMAN);	On-premise	NO DOWNTIME		
2	Creazione pfile (parameter file) a partire dal spfile (server parameter file) del DB AS-IS;	On-premise			
3	Export password file del DB AS-IS;	On-premise			
4	Trasferimento del wallet dall'AS-IS verso il TO-BE per decriptazione backup;	On-premise/PSN			
5	Startup DB TO-BE con opzione NOMOUNT e con pfile (opportunamente modificato);	PSN			
6	Restore controlfile su DB TO-BE;	PSN			
7	Restore e recover del DB su ambiente TO-BE.	PSN			

Tabella 339 - Drilldown RMAN

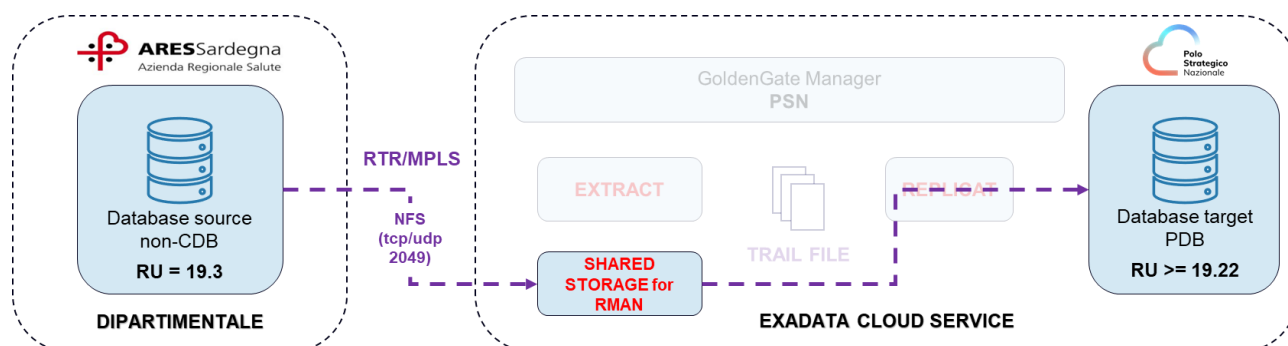


Figura 20 - Strategia di Migrazione - Golden Gate – Primo import datai da eseguire con RMAN.

N.B: Lo shared storage sarà predisposto all'interno del perimetro ExaCS e dovrà necessariamente essere visibile (mount NFS) direttamente ai DB dei dipartimentali.

La migrazione richiede il soddisfacimento di una serie di prerequisiti, che sono dettagliatamente elencati nella tabella seguente. Questi prerequisiti comprendono tutte le condizioni necessarie per garantire una transizione fluida e senza interruzioni, sia a livello infrastrutturale che operativo, assicurando così il corretto funzionamento del sistema durante e dopo il processo di migrazione.

ID	Task	Ambiente	Owner	Vincoli
1	Acquisto licenza Golden Gate.	N/A	ARES	Acquisto declinato all'Amm.ne
2	GG - Configurazione networking RTR (regole FW, Natting, etc.) tra il singolo dipartimentale e il PSN per replica dati.	PSN	SardegnaIT	Connettività MPLS
3	GG - Configurazione networking MPLS (regole FW, Natting, etc.) tra il singolo dipartimentale e il PSN per replica dati.	On-premise/PSN	SardegnaIT/LDO	Connettività MPLS
4	RMAN - Configurazione networking RTR (regole FW, Natting, etc.) tra il singolo dipartimentale e il PSN per mount NFS shared storage.	On-premise/PSN	SardegnaIT	Connettività MPLS
5	RMAN - Configurazione networking MPLS (regole FW, Natting, etc.) tra il singolo dipartimentale e il PSN per mount NFS shared storage.	On-premise/PSN	SardegnaIT/LDO	Connettività MPLS
6	Configurazione GoldenGate ambiente AS-IS (dipartimentali)*.	On-premise	ARES/Fornitore	Accesso ambiente on-premise
7	Predisposizione ExaCS, rilascio risorse e abilitazione accessi.	PSN	PSN/TIM	Accesso ambiente target PSN
8	Configurazione infrastruttura ExaCS (VM, GRID, DB, Network, Storage, etc..)*	PSN	PSN/ACN	Accesso ambiente target PSN
9	Configurazione GoldenGate ambiente TO-BE (PSN ExaCS)*.	PSN	PSN/ACN	Accesso ambiente target PSN

Tabella 340 - Prerequisiti migrazione con Oracle Golden Gate

* Attività non previste in fase di progetto del piano dei fabbisogni.

1. Verifiche consistenza/Integrità dati tramite RMAN (Recovery Manager)

RMAN è lo strumento di backup e ripristino per database Oracle che verrà utilizzato come strumento di migrazione per eseguire il primo import (initial load) dei database dipartimentali Sisar. Può anche verificare l'integrità dei dati durante una migrazione. Le attività di verifica con RMAN includono:

- **Backup e ripristino (Backup & Restore):** Durante il ripristino, RMAN verifica automaticamente l'integrità dei dati. Il processo di backup performa in background un checksum per ogni singolo blocco e lo salva nel backup, che viene verificato automaticamente durante il ripristino.

- **Controllo Integrità dei backup (RMAN Validation):** Tramite il comando **VALIDATE** di RMAN, è possibile verificare che i backup siano integri e che non ci siano blocchi fisici corrotti (Media corruption).
- **Controllo dei blocchi logici corrotti:** Di default, il comando **VALIDATE** controlla solo la corruzione fisica dei dati. Utilizzando il comando **BACKUP VALIDATE CHECK LOGICAL**, è possibile identificare eventuali blocchi logici corrotti nel database di origine prima della migrazione. Esempi di corruzione logica, includono dati corrotti a livello di record (row piece) o indici (index entry).
- **Verifica dei dati post ripristino:** Dopo il ripristino del database, il comando **RESTORE VALIDATE DATABASE** viene utilizzato per assicurarsi che tutti i dati siano stati ripristinati correttamente.

Link Riferimento: [Validating Database Files and Backups](#)

2. Verifiche di latenza/integrità transazionale con GoldenGate

Successivamente, Oracle Golden Gate verrà utilizzato Oracle GoldenGate come strumento di replica dei dati in tempo reale. È un prodotto efficace per migrazioni con tempi di inattività minimi, come la migrazione dei DB Sisar. Le attività di verifica con Golden Gate includono:

- **Controllo della latenza:** Oracle GoldenGate monitora la latenza della replica in tempo reale per assicurarsi che le modifiche vengono replicate rapidamente dal sistema sorgente a quello di destinazione.
- **Convalida della replica:** Durante la replica, GoldenGate garantisce l'integrità transazionale (solo le transazioni committate vengono replicate) e verifica che tutte le transazioni siano applicate correttamente.

Link Riferimento: [Replica e trasformazione dei dati](#) | [Oracle GoldenGate](#) | [Oracle Italia](#)

5.3.2 Primo Mock

Task	Ambiente	Durata	Owner	Vincoli
Primo backup full del database attualmente in produzione. Rilevazione del tempo necessario all'operazione.	On-premise	TBD	Athena	N/A
Trasferimento del backup full sulla shared folder del PSN. Rilevazione del tempo necessario all'operazione.	On-premise to PSN	TDB	Athena	N/A
Restore del database sulla nuova infrastruttura Oracle ExaCS del PSN. Rilevazione del tempo necessario all'operazione.	PSN	TDB	ACN	N/A

Tabella 341 - Primo mock

6 COLLAUDO

In questa fase viene predisposto un ambiente di collaudo (test plant) sull'ambiente target ed eseguiti i test previsti seguendo la schedulazione concordata con l'Amministrazione.

L'esito dei test sarà registrato in appositi report concordati con l'Amministrazione.

Nei paragrafi successivi sono riportati i test (UAT = User Acceptance Test) di disponibilità, integrità e funzionalità previsti a seguito della migrazione su PSN delle piattaforme applicative.

6.1 Test List Piattaforma Applicativa SISaR

ID UAT	RAG01_SIO
Nome del test	Verifica raggiungibilità sistemi SIO
Prerequisiti	N/A
Input	Indirizzo sistema bilanciato target
Output atteso	Raggiungibilità maschera di accesso
ID UAT	RAG01_AAP
Nome del test	Verifica raggiungibilità sistemi AAP
Prerequisiti	N/A
Input	Indirizzo sistema bilanciato target
Output atteso	Raggiungibilità maschera di accesso
ID UAT	FUN02_SIO
Nome del test	Verifica funzionalità sistemi SIO
Prerequisiti	RAG01_SIO con esito Positivo
Input	Test specifici su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	FUN02_AAP
Nome del test	Verifica funzionalità sistemi AAP
Prerequisiti	RAG01_AAP con esito Positivo
Input	Test specifici su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	PER03_SIO
Nome del test	Verifica performance sistemi SIO
Prerequisiti	FUN02_SIO con esito Positivo
Input	Test specifici su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	PER03_AAP
Nome del test	Verifica performance sistemi AAP

Prerequisiti	FUN02_AAP con esito Positivo
Input	Test specifici su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	INT04_SIO
Nome del test	Verifica integrazioni sistemi SIO
Prerequisiti	FUN02_SIO con esito Positivo
Input	Test specifici di integrazione su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	INT04_AAP
Nome del test	Verifica integrazioni sistemi SIO
Prerequisiti	FUN02_AAP con esito Positivo
Input	Test specifici di integrazione su singoli moduli e funzionalità
Output atteso	Risultati in linea con sistema sorgente
ID UAT	FUN02_SIO_ACCESSEO
Nome del test	Accesso al sistema
Prerequisiti	RAG01_SIO con esito positivo
Input	Nome utente e password applicativa
Output atteso	Scelta della configurazione Azienda, Ufficio, Ruolo
ID UAT	FUN02_SIO_LDA01
Nome del test	Ricerca assistito
Prerequisiti	FUN02_SIO_ACCESSEO con esito Positivo
Input	Codice Fiscale
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_LDA02
Nome del test	Aggiornamento dati anagrafici
Prerequisiti	FUN02_SIO_LDA01 con esito Positivo
Input	Indirizzo domicilio e numero di telefono
Output atteso	Aggiornamento effettuato con successo
ID UAT	FUN02_SIO_LDA03
Nome del test	Registrazione Prenotazione in linea
Prerequisiti	FUN02_SIO_LDA02 con esito Positivo
Input	Reparto di Ricovero e diagnosi
Output atteso	Registrazione effettuata con successo e generazione identificativo di prenotazione
ID UAT	FUN02_SIO_LDA04
Nome del test	Inserimento Pre-Ricovero
Prerequisiti	FUN02_SIO_LDA03 con esito Positivo
Input	Data Inizio Pre-Ricovero

Output atteso	Registrazione effettuata con successo e scrittura su tabelle di frontiera per messagistica ADT
ID UAT	FUN02_SIO_LDA05
Nome del test	Convocazione Assistito
Prerequisiti	FUN02_SIO_LDA03 con esito Positivo
Input	Data Convocazione + Esito (Accetta/Rifiuta)
Output atteso	Registrazione effettuata con successo
ID UAT	FUN02_SIO_ADT01.1
Nome del test	Ricerca Assistiti Convocati in LDA
Prerequisiti	FUN02_SIO_LDA05 con esito Positivo
Input	Codice Fiscale + Stato = "In lista di attesa"
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_ADT01.2
Nome del test	Ricerca Assistiti in stato "Da Ammettere"
Prerequisiti	FUN02_SIO_PS06.2 con esito Positivo
Input	Codice Fiscale + Stato = "Da Ammettere" + Reparto Ricovero
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_ADT02
Nome del test	Registrazione Ricovero Ordinario
Prerequisiti	FUN02_SIO_ADT01 con esito Positivo oppure FUN02_SIO_PS09.2 con esito Positivo
Input	Campi obbligatori
Output atteso	Registrazione effettuata con successo; generazione nosologico; scrittura su tabelle di frontiera per messagistica ADT
ID UAT	FUN02_SIO_ADT03
Nome del test	Trasferimento Paziente
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo
Input	Reparto di Destinazione
Output atteso	Registrazione effettuata con successo; scrittura su tabelle di frontiera per messagistica ADT
ID UAT	FUN02_SIO_ADT04
Nome del test	Import Diagnosi e Interventi "Da Blocco Ospedaliero"
Prerequisiti	FUN02_SIO_SOWEB05 con esito positivo
Input	Diagnosi "Da Blocco Ospedaliero" e Interventi "Da Blocco Ospedaliero"
Output atteso	Diagnosi e Interventi importati con successo
ID UAT	FUN02_SIO_ADT05
Nome del test	Richiesta Esami Consulenza
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo

Input	Prestazione + Erogatore
Output atteso	Inoltro Richiesta; Stampa modulo consulenza
ID UAT	FUN02_SIO_ADT06
Nome del test	Certificato INPS
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo
Input	Compilazione Dati Obbligatori
Output atteso	Registrazione certificato avvenuta con successo
ID UAT	FUN02_SIO_ADT07
Nome del test	Dimissione paziente
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo
Input	Data/ora dimissione + Esito Ricovero
Output atteso	Dimissione effettuata con successo; Creazione LDO secondo specifiche attive; scrittura su tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_ADT08
Nome del test	Validazione Ricovero
Prerequisiti	FUN02_SIO_ADT06 con esito Positivo
Input	Cliccare sul bottone Valida
Output atteso	Verifica delle regole di validazione e storicizzazione ricovero
ID UAT	FUN02_SIO_CCA01.1
Nome del test	Ricerca Paziente da Pianificare (Paziente interno: Order Entry)
Prerequisiti	FUN02_SIO_ADT05 con esito Positivo
Input	Codice Fiscale
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_CCA01.2
Nome del test	Ricerca Paziente Pianificato (Paziente esterno: CUPWeb)
Prerequisiti	Registrazione Richiesta CUP con esito Positivo
Input	Ambulatorio Erogatore, Data e ora appuntamento
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_CCA02
Nome del test	Pianifica Consulenza
Prerequisiti	FUN02_SIO_CCA01 con esito Positivo
Input	Data e ora appuntamento
Output atteso	Pianificazione avvenuta con successo
ID UAT	FUN02_SIO_CCA03
Nome del test	Presa in carico paziente
Prerequisiti	FUN02_SIO_CCA02 con esito Positivo
Input	Apertura Cartella

Output atteso	Registrazione identificativo Cartella e Contatto
ID UAT	FUN02_SIO_CCA04
Nome del test	Erogazione Visita
Prerequisiti	FUN02_SIO_CCA03 con esito Positivo
Input	Compilazione Checklist di refertazione + Validazione Referto
Output atteso	Generazione Referto secondo specifiche attive
ID UAT	FUN02_SIO_CCA05
Nome del test	Certificato INPS
Prerequisiti	FUN02_SIO_CCA03 con esito Positivo
Input	Compilazione Campi obbligatori
Output atteso	Registrazione Certificato
ID UAT	FUN02_SIO_PS01
Nome del test	Ricerca assistito
Prerequisiti	FUN02_SIO_ACCESO con esito Positivo
Input	Codice Fiscale
Output atteso	Risultato della ricerca
ID UAT	FUN02_SIO_PS02.1
Nome del test	Registrazione Triage
Prerequisiti	FUN02_SIO_PS01 con esito Positivo
Input	Priorità Ingresso + Campi obbligatori
Output atteso	Registrazione avvenuta con successo; generazione id univoco PS; Inserimento paziente in lista; Scrittura nelle tabelle di frontiera per messaggistica ADT; Ribaltamento info su Diario Clinico
ID UAT	FUN02_SIO_PS02.2
Nome del test	Associazione missione 118
Prerequisiti	FUN02_SIO_PS01 con esito Positivo; INT04_SIO_PS01 con esito Positivo
Input	Codice Missione
Output atteso	Associazione accesso PS - missione 118; Scrittura in tabelle di frontiera per comunicazione alle CO118 della registrazione paziente
ID UAT	FUN02_SIO_PS03
Nome del test	Presa in carico paziente
Prerequisiti	FUN02_SIO_PS02 con esito Positivo
Input	Ambulatorio
Output atteso	Cambio Stato; Apertura Cartella; Ribaltamento info su Diario Clinico; Scrittura nelle tabelle di frontiera per messaggistica ADT; Scrittura in tabelle di frontiera per comunicazione alle CO118 della presa in carico
ID UAT	FUN02_SIO_PS04.1

Nome del test	Compilazione Certificato medico di infortunio
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Campi obbligatori
Output atteso	Registrazione Certificato
ID UAT	FUN02_SIO_PS04.2
Nome del test	Compilazione Certificato medico di malattia (INPS)
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Campi obbligatori
Output atteso	Registrazione Certificato
ID UAT	FUN02_SIO_PS05
Nome del test	Parametri Vitali
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Inserimento Valori
Output atteso	Registrazione Parametri Vitali; Ribaltamento info su Diario Clinico
ID UAT	FUN02_SIO_PS06.1
Nome del test	Dimissione Paziente a Domicilio
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Diagnosi dimissione + Esito PS
Output atteso	Dimissione effettuata con successo; Generazione VPS secondo specifiche attive; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS06.2
Nome del test	Dimissione Paziente verso Ricovero Ospedaliero
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Diagnosi dimissione + Esito PS
Output atteso	Dimissione effettuata con successo; Generazione VPS secondo specifiche attive; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS06.3
Nome del test	Dimissione Paziente in OBI
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Diagnosi dimissione OBI + Esito PS
Output atteso	Dimissione effettuata con successo; Generazione VPS secondo specifiche attive; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS07
Nome del test	Registrazione Paziente in OBI
Prerequisiti	FUN02_SIO_PS06.3 con esito Positivo
Input	Stanza - Letto

Output atteso	Assegnazione PL; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS08
Nome del test	Gestione Paziente in OBI
Prerequisiti	FUN02_SIO_PS07 con esito Positivo
Input	Apertura Cartella OBI
Output atteso	Generazione identificativo univoco accesso OBI; scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS09.1
Nome del test	Dimissione Paziente in OBI
Prerequisiti	FUN02_SIO_PS08 con esito Positivo
Input	Esito Dimissione Domicilio
Output atteso	Dimissione avvenuta con successo; Stampa VPS OBI; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_PS09.2
Nome del test	Dimissione Paziente in OBI
Prerequisiti	FUN02_SIO_PS08 con esito Positivo
Input	Esito Dimissione Ricovero Ospedaliero
Output atteso	Dimissione avvenuta con successo; Stampa VPS OBI; Scrittura nelle tabelle di frontiera per messaggistica ADT
ID UAT	FUN02_SIO_SOWEB01.1
Nome del test	Ricerca paziente in lista d'attesa
Prerequisiti	FUN02_SIO_LDA03 con esito Positivo
Input	Codice Fiscale
Output atteso	Risultato della Ricerca
ID UAT	FUN02_SIO_SOWEB01.2
Nome del test	Ricerca paziente da Ricovero Ospedaliero
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo
Input	Codice Fiscale
Output atteso	Risultato della Ricerca
ID UAT	FUN02_SIO_SOWEB02
Nome del test	Registrazione Proposta Operatoria
Prerequisiti	FUN02_SIO_SOWEB01 con esito Positivo
Input	Codice Fiscale + Agenda
Output atteso	Registrazione Paziente in lista Operatoria avvenuta con successo
ID UAT	FUN02_SIO_SOWEB03
Nome del test	Registrazione Atto Operatorio
Prerequisiti	FUN02_SIO_SOWEB02 con esito Positivo
Input	Campi Obbligatori

Output atteso	Atto operatorio registrato correttamente; Generazione identificativo univoco.
ID UAT	FUN02_SIO_SOWEB04
Nome del test	Compilazione Cartella Infermieristica
Prerequisiti	FUN02_SIO_SOWEB03 con esito Positivo
Input	Campi Obbligatori
Output atteso	Cartella infermieristica registrata correttamente
ID UAT	FUN02_SIO_SOWEB04
Nome del test	Compilazione Cartella Anestesista
Prerequisiti	FUN02_SIO_SOWEB03 con esito Positivo
Input	Campi Obbligatori
Output atteso	Cartella Anestesista registrata correttamente
ID UAT	FUN02_SIO_SOWEB05
Nome del test	Registrazione Diagnosi e Interventi
Prerequisiti	FUN02_SIO_SOWEB03 con esito Positivo
Input	Campi Obbligatori
Output atteso	Diagnosi e Interventi registrati correttamente
ID UAT	FUN02_SIO_SOWEB06
Nome del test	Registrazione Materiali e Protesi
Prerequisiti	FUN02_SIO_SOWEB03 con esito Positivo
Input	Campi Obbligatori
Output atteso	Materiali e Protesi registrati correttamente;
ID UAT	FUN02_SIO_SOWEB07
Nome del test	Registrazione Equipe Intervento
Prerequisiti	FUN02_SIO_SOWEB04 con esito Positivo
Input	Campi Obbligatori
Output atteso	Equipe registrata correttamente
ID UAT	FUN02_SIO_SOWEB08
Nome del test	Chiusura Atto Operatorio
Prerequisiti	FUN02_SIO_SOWEB06 con esito Positivo
Input	Campi Obbligatori
Output atteso	Chiusura Atto Operatorio; Stampa Registro Operatorio; Scarico Materiali e Protesi verso magazzino AMC; Scarico diagnosi e interventi verso ADTWeb.
ID UAT	FUN02_AAP_ACCESO
Nome del test	Accesso al sistema
Prerequisiti	RAG01_AAP con esito Positivo
Input	Nome utente e password applicativa
Output atteso	Scelta della configurazione Azienda, Ufficio, Ruolo

ID UAT	FUN02_AAP_CSS01
Nome del test	Ricerca assistito
Prerequisiti	FUN02_AAP_ACCESSO con esito Positivo
Input	Cognome e data nascita
Output atteso	Risultato della ricerca
ID UAT	FUN02_AAP_CSS02
Nome del test	Aggiornamento dati sociosanitari
Prerequisiti	FUN02_AAP_CSS01 con esito Positivo
Input	Titolo di studio
Output atteso	Aggiornamento effettuato con successo
ID UAT	FUN02_AAP_CSS03
Nome del test	Creazione nuova pratica PUA
Prerequisiti	FUN02_AAP_CSS02 con esito Positivo
Input	Azione sul bottone PUA presente nella scheda Elenco pratiche
Output atteso	Apertura modulo PUA
ID UAT	FUN02_AAP_PUA01
Nome del test	Creazione nuova pratica PUA
Prerequisiti	FUN02_AAP_CSS03 con esito Positivo
Input	Compilazione dati obbligatori sulla scheda di contatto
Output atteso	Creazione pratica e rilascio protocollo progressivo
ID UAT	FUN02_AAP_PUA02
Nome del test	Compilazione valutazione di primo livello
Prerequisiti	FUN02_AAP_PUA01 con esito Positivo
Input	Inserimento di almeno una scheda di valutazione
Output atteso	Creazione di 1 di N record all'interno della tabella delle valutazioni
ID UAT	FUN02_AAP_PUA03
Nome del test	Compilazione scheda di prevalutazione
Prerequisiti	FUN02_AAP_PUA01 con esito Positivo
Input	Compilazione di almeno un campo della scheda
Output atteso	Aggiornamento scheda di prevalutazione
ID UAT	FUN02_AAP_PUA04
Nome del test	Compilazione patologie
Prerequisiti	FUN02_AAP_PUA01 con esito Positivo
Input	Inserimento della patologia prevalente obbligatoria e di almeno una concomitante
Output atteso	Aggiornamento patologie
ID UAT	FUN02_AAP_PUA05
Nome del test	Compilazione unità di valutazione

Prerequisiti	FUN02_AAP_PUA01 con esito Positivo
Input	Inserimento dei dati obbligatori e con esito verbale UVT positivo
Output atteso	Aggiornamento unità di valutazione e abilitazione scheda progetto
ID UAT	FUN02_AAP_PUA06.1
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA05 con esito Positivo
Input	Inserimento progetto cure domiciliari
Output atteso	Aggiornamento progetto con servizio cure domiciliari nella sezione dedicata
ID UAT	FUN02_AAP_PUA06.2
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA05 con esito Positivo
Input	Inserimento progetto RSA
Output atteso	Aggiornamento progetto con servizio RSA nella sezione dedicata
ID UAT	FUN02_AAP_PUA06.3
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA05 con esito Positivo
Input	Inserimento progetto Hospice
Output atteso	Aggiornamento progetto con servizio Hospice nella sezione dedicata
ID UAT	FUN02_AAP_PUA06.4
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA05 con esito Positivo
Input	Inserimento progetto Protesica - Integrativa
Output atteso	Aggiornamento progetto con servizio Protesica - Integrativa nella sezione dedicata
ID UAT	FUN02_AAP_PUA06.5
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA06.1 con esito Positivo
Input	Inserimento dati obbligatori servizio cure domiciliari e conferma creazione pratica
Output atteso	Creazione pratica ADI
ID UAT	FUN02_AAP_PUA06.6
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA06.2 con esito Positivo
Input	Inserimento dati obbligatori servizio RSA e conferma creazione pratica
Output atteso	Creazione pratica RSA
ID UAT	FUN02_AAP_PUA06.7

Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA06.3 con esito Positivo
Input	Inserimento dati obbligatori servizio Hospice e conferma creazione pratica
Output atteso	Creazione pratica Hospice
ID UAT	FUN02_AAP_PUA06.8
Nome del test	Compilazione progetto
Prerequisiti	FUN02_AAP_PUA06.4 con esito Positivo
Input	Inserimento dati obbligatori servizio Protesica - Integrativa e conferma creazione pratica
Output atteso	Creazione pratica Protesica
ID UAT	FUN02_AAP_ADI01
Nome del test	Compilazione scheda contatto cure domiciliari
Prerequisiti	FUN02_AAP_PUA06 con esito Positivo
Input	Inserimento dati obbligatori e verifica dati ereditati dal PUA
Output atteso	Aggiornamento scheda contatto cure domiciliari
ID UAT	FUN02_AAP_ADI02
Nome del test	Verifica patologie
Prerequisiti	FUN02_AAP_ADI01 con esito Positivo
Input	Apertura scheda patologie
Output atteso	Presenza delle patologie inserite sul PUA
ID UAT	FUN02_AAP_ADI03
Nome del test	Verifica unità valutativa
Prerequisiti	FUN02_AAP_ADI01 con esito Positivo
Input	Apertura scheda unità valutativa
Output atteso	Presenza delle informazioni e schede di valutazione inserita sul PUA
ID UAT	FUN02_AAP_ADI04
Nome del test	Compilazione del PAI
Prerequisiti	FUN02_AAP_ADI03 con esito Positivo
Input	Inserimento interventi nel piano assistenziale individuale
Output atteso	Calendarizzazione interventi programmati per prestazione e figura professionale
ID UAT	FUN02_AAP_RSA01
Nome del test	Compilazione scheda contatto RSA
Prerequisiti	FUN02_AAP_PUA06.2 con esito Positivo
Input	Inserimento dati obbligatori e verifica dati ereditati dal PUA
Output atteso	Aggiornamento scheda contatto RSA
ID UAT	FUN02_AAP_RSA02
Nome del test	Verifica patologie

Prerequisiti	FUN02_AAP_RSA01 con esito Positivo
Input	Apertura scheda patologie
Output atteso	Presenza delle patologie inserite sul PUA
ID UAT	FUN02_AAP_RSA03
Nome del test	Verifica unità valutativa
Prerequisiti	FUN02_AAP_RSA01 con esito Positivo
Input	Apertura scheda unità valutativa
Output atteso	Presenza delle informazioni e schede di valutazione inserita sul PUA
ID UAT	FUN02_AAP_RSA04
Nome del test	Compilazione progetto assistenziale
Prerequisiti	FUN02_AAP_RSA03 con esito Positivo
Input	Inserimento dati obbligatori, tra cui la struttura di ricovero
Output atteso	Aggiornamento progetto assistenziale e preparazione ricovero
ID UAT	FUN02_AAP_RSA05
Nome del test	Ricovero presso struttura residenziale o semiresidenziale
Prerequisiti	FUN02_AAP_RSA04 con esito Positivo
Input	Inserimento data ricovero e livello assistenziale
Output atteso	Conferma del ricovero
ID UAT	FUN02_AAP_HOS01
Nome del test	Compilazione scheda contatto Hospice
Prerequisiti	FUN02_AAP_PUA06.3 con esito Positivo
Input	Inserimento dati obbligatori e verifica dati ereditati dal PUA
Output atteso	Aggiornamento scheda contatto Hospice
ID UAT	FUN02_AAP_HOS02
Nome del test	Verifica patologie e inserimento segni sintomi clinici
Prerequisiti	FUN02_AAP_HOS01 con esito Positivo
Input	Apertura scheda patologie
Output atteso	Presenza delle patologie inserite sul PUA e inserimento segni sincomi clinici
ID UAT	FUN02_AAP_HOS03
Nome del test	Verifica unità valutativa
Prerequisiti	FUN02_AAP_HOS01 con esito Positivo
Input	Apertura scheda unità valutativa
Output atteso	Presenza delle informazioni e schede di valutazione inserita sul PUA
ID UAT	FUN02_AAP_HOS04
Nome del test	Compilazione progetto assistenziale
Prerequisiti	FUN02_AAP_HOS03 con esito Positivo

Input	Inserimento dati obbligatori, tra cui la struttura di ricovero
Output atteso	Aggiornamento progetto assistenziale e preparazione ricovero
ID UAT	FUN02_AAP_HOS05
Nome del test	Ricovero presso struttura Hospice
Prerequisiti	FUN02_AAP_RSA04 con esito Positivo
Input	Inserimento data ricovero
Output atteso	Conferma del ricovero
ID UAT	FUN02_AAP_PRO01
Nome del test	Compilazione scheda di contatto Protesica
Prerequisiti	FUN02_AAP_PUA06.8 con esito Positivo
Input	Inserimento dati obbligatori e verifica dati ereditati dal PUA
Output atteso	Aggiornamento scheda di ricovero
ID UAT	FUN02_AAP_PRO02
Nome del test	Gestione dispositivi
Prerequisiti	FUN02_AAP_PRO01 con esito Positivo
Input	Codici ISO e tipologia fornitura
Output atteso	Aggiornamento tabella dispositivi con relativa fornitura
ID UAT	FUN02_AAP_PRO03
Nome del test	Autorizzazione pratica protesica
Prerequisiti	FUN02_AAP_PRO02 con esito Positivo
Input	Autorizzazione dispositivi selezionati
Output atteso	Cambio stato pratica in Autorizzata
ID UAT	FUN02_AAP_PRO04
Nome del test	Consegna certificato autorizzativo
Prerequisiti	FUN02_AAP_PRO03 con esito Positivo
Input	Azione su bottone segnala consegna certificato
Output atteso	Aggiornamento della data della consegna certificato autorizzativo
ID UAT	FUN02_AAP_PRO05
Nome del test	Completamento pratica
Prerequisiti	FUN02_AAP_PRO04 con esito Positivo
Input	Inserimento fornitore e azione sul bottone Completa pratica
Output atteso	Cambio stato pratica in Completata
ID UAT	FUN02_AAP_PRO06
Nome del test	Completamento pratica
Prerequisiti	FUN02_AAP_PRO05 con esito Positivo
Input	Inserimento fornitore e azione sul bottone Completa pratica
Output atteso	Cambio stato pratica in Completata

ID UAT	FUN02_AAP_PRO07
Nome del test	Consegna pratica
Prerequisiti	FUN02_AAP_PRO06 con esito Positivo
Input	Inserimento data consegna, bolla e azione su bottone Consegna
Output atteso	Cambio stato pratica dei dispositivi in consegnati
ID UAT	FUN02_AAP_ML01
Nome del test	Accesso modulo Medicina Legale
Prerequisiti	FUN02_AAP_ACCESSO con esito Positivo
Input	Azione su bottone Medicina Legale
Output atteso	Apertura modulo Medicina Legale
ID UAT	FUN02_AAP_ML02
Nome del test	Certificati semplici
Prerequisiti	FUN02_AAP_ML01 con esito Positivo
Input	Inserimento certificato semplice con i dati obbligatori
Output atteso	Generazione certificato semplice
ID UAT	FUN02_AAP_ML03
Nome del test	Gestione verbale di invalidità civile
Prerequisiti	FUN02_AAP_ML01 con esito Positivo
Input	Inserimento dati obbligatori previsti per l'invalidità civile
Output atteso	Generazione verbale di invalidità civile
ID UAT	FUN02_AAP_ML04
Nome del test	Gestione verbale di handicap
Prerequisiti	FUN02_AAP_ML01 con esito Positivo
Input	Inserimento dati obbligatori previsti per l'handicap
Output atteso	Generazione verbale di handicap
ID UAT	FUN02_AAP_CON01
Nome del test	Accesso modulo Consultorio
Prerequisiti	FUN02_AAP_ACCESSO con esito Positivo
Input	Inserimento dati obbligatori per accesso consultoriale
Output atteso	Apertura cartella consultoriale
ID UAT	FUN02_AAP_CON02
Nome del test	Compilazione anamnesi
Prerequisiti	FUN02_AAP_CON01 con esito Positivo
Input	Inserimento dati su scheda anamnestica
Output atteso	Aggiornamento anamnesi assistito
ID UAT	FUN02_AAP_CON03
Nome del test	Compilazione valutazioni
Prerequisiti	FUN02_AAP_CON01 con esito Positivo

Input	Inserimento dati su scheda valutazioni
Output atteso	Aggiornamento valutazioni assistito
ID UAT	FUN02_AAP_CON04
Nome del test	Compilazione impegnativa
Prerequisiti	FUN02_AAP_CON01 con esito Positivo
Input	Inserimento impegnativa
Output atteso	Generazione impegnativa
ID UAT	FUN02_AAP_CON05
Nome del test	Gestione prestazioni
Prerequisiti	FUN02_AAP_CON01 con esito Positivo
Input	Inserimento di almeno una prestazione
Output atteso	Elenco prestazioni effettuate all'assistito
ID UAT	FUN02_AAP_CON06
Nome del test	Refertazione
Prerequisiti	FUN02_AAP_CON05 con esito Positivo
Input	Inserimento dati di sintesi
Output atteso	Generazione del referto
ID UAT	INT04_AAP_PUA01
Nome del test	Integrazione ADT-PUA
Prerequisiti	Invio dimissione concordata ad ADT
Input	Azione su bottone crea pratica da segnalazioni dall'ospedale
Output atteso	Creazione pratica PUA
ID UAT	INT04_AAP_ADI01
Nome del test	Acquisizione accessi effettuati
Prerequisiti	Invio PAI ad un fornitore terzo e ricezione lor interventi
Input	PAI in corso
Output atteso	Cambio stato interventi da assegnato a effettuato
ID UAT	INT04_AAP_PROTE01
Nome del test	Invio ordine verso AMC
Prerequisiti	Raggiungibilità del sistema AMC e integrazione attiva
Input	Data ordine e azione su bottone completa pratica
Output atteso	Identificativo ordine AMC
ID UAT	INT04_AAP_PROTE02
Nome del test	Invio movimento di carico verso AMC
Prerequisiti	INT04_AAP_PROTE01 con esito Positivo
Input	Data consegna e bolla
Output atteso	Identificativo consegna AMC
ID UAT	INT04_AAP_ML01

Nome del test	Scarico domande da NPS
Prerequisiti	Raggiungibilità servizi di cooperazione applicativa INPS
Input	Azione su bottone scarico domande
Output atteso	Lista delle domande INPS
ID UAT	INT04_AAP_ML02
Nome del test	Invio verbale invalidità civile ad INPS
Prerequisiti	INT04_AAP_ML01 con esito Positivo
Input	Azione su invio verbale
Output atteso	Ricezione esito positivo di avvenuta accettazione dai sistemi INPS
ID UAT	INT04_AAP_ML03
Nome del test	Ricezione esito verbale invalidità civile ad INPS
Prerequisiti	INT04_AAP_ML02 con esito Positivo
Input	Azione su scarica esiti
Output atteso	Ricezione esito definitivo da INPS
ID UAT	INT04_AAP_ML04
Nome del test	Invio verbale handicap ad INPS
Prerequisiti	INT04_AAP_ML01 con esito Positivo
Input	Azione su invio verbale
Output atteso	Ricezione esito positivo di avvenuta accettazione dai sistemi INPS
ID UAT	INT04_AAP_ML05
Nome del test	Ricezione esito verbale handicap ad INPS
Prerequisiti	INT04_AAP_ML0 con esito Positivo
Input	Azione su scarica esiti
Output atteso	Ricezione esito definitivo da INPS
ID UAT	INT04_SIO_LDA01
Nome del test	Invio Accesso Pre-Ricovero a Sistemi Terzi tramite messagistica ADT_A01
Prerequisiti	Registrazione Pre-ricovero
Input	Data e Ora Pre-ricovero e conferma
Output atteso	Inserimento Pre-ricovero e scrittura nelle tabelle di frontiera del messaggio ADT_A01
ID UAT	INT04_SIO_LDA02
Nome del test	Cancellazione Accesso Pre-Ricovero a Sistemi Terzi tramite messagistica ADT_A38
Prerequisiti	Cancellazione Pre-ricovero
Input	Sbianco Data e Ora Pre-ricovero e conferma
Output atteso	Cancellazione Pre-ricovero e scrittura nelle tabelle di frontiera del messaggio ADT_A38
ID UAT	INT04_SIO_ADT01

Nome del test	Invio Accesso in reparto a Sistemi Terzi tramite messagistica ADT_A01
Prerequisiti	FUN02_SIO_ADT02 con esito Positivo
Input	Compilare dati obbligatori e conferma
Output atteso	Registrazione ricovero e scrittura nelle tabelle di frontiera del messaggio ADT_A01
ID UAT	INT04_SIO_ADT02
Nome del test	Invio Trasferimento Ricovero a Sistemi Terzi tramite messagistica ADT_A02
Prerequisiti	FUN02_SIO_ADT03 con esito Positivo
Input	Registro reparto di destinazione e conferma
Output atteso	Registro trasferimento e scrittura nelle tabelle di frontiera del messaggio ADT_A02
ID UAT	INT04_SIO_ADT03
Nome del test	Richiesta di Consulenza
Prerequisiti	FUN02_SIO_ADT03 con esito Positivo
Input	Registro richiesta e conferma
Output atteso	Richiesta disponibile nel piano di lavoro ambulatoriale
ID UAT	INT04_SIO_ADT03
Nome del test	Richiesta di Consulenza
Prerequisiti	FUN02_SIO_ADT03 con esito Positivo
Input	Registro richiesta e conferma inoltro
Output atteso	Stampa automatica modulo; Richiesta disponibile nel piano di lavoro ambulatoriale
ID UAT	INT04_SIO_ADT03
Nome del test	Richiesta di Consulenza
Prerequisiti	FUN02_SIO_ADT03 con esito Positivo
Input	Registro richiesta e conferma inoltro
Output atteso	Stampa automatica modulo; Richiesta disponibile nel piano di lavoro ambulatoriale
ID UAT	INT04_SIO_ADT04
Nome del test	Invio Certificato Inps
Prerequisiti	FUN02_SIO_ADT06 con esito Positivo
Input	Compilazione e conferma inoltro
Output atteso	Ricevuta Inps: n. protocollo
ID UAT	INT04_SIO_ADT05
Nome del test	Invio LDO a FSE
Prerequisiti	FUN02_SIO_ADT07 con esito Positivo
Input	Validazione LDO
Output atteso	Generazione documento e trasmissione a FSE
ID UAT	INT04_SIO_PS01

Nome del test	Invio Richiesta Radiologica
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Compilazione e conferma inoltro
Output atteso	Stampa Automatica modulo; Richiesta disponibile nel piano di lavoro RIS/CIS
ID UAT	INT04_SIO_PS02
Nome del test	Certificato INAIL
Prerequisiti	FUN02_SIO_PS04.1 con esito Positivo
Input	Compilazione e conferma inoltro
Output atteso	Ricevuta INAIL: n. protocollo + Codice Sede Competenza
ID UAT	INT04_SIO_PS03
Nome del test	Ricezione Pre-Allerte
Prerequisiti	FUN02_SIO con esito Positivo
Input	-
Output atteso	Risultato Ricerca: preallerte disponibili nella funzionalità dedicata
ID UAT	INT04_SIO_PS04
Nome del test	Calcolo Importo Ticket
Prerequisiti	FUN02_SIO_PS09 con esito Positivo
Input	Dimissione con codice verde e causa accettazione diversa da trauma
Output atteso	Calcolo importo ticket e comunicazione a CUPWeb per disposizione pagamento
ID UAT	INT04_SIO_PS05
Nome del test	Invio VPS a FSE
Prerequisiti	FUN02_SIO_PS09 con esito Positivo
Input	Dimissione Paziente
Output atteso	Generazione documento e trasmissione a FSE
ID UAT	INT04_SIO_PS06
Nome del test	Inserimento Richiesta Trasfusionale
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Prestazioni Trasfusionali: profilo sconosciuto
Output atteso	Invio richiesta; stampa automatica etichette e modulo
ID UAT	INT04_SIO_PS07
Nome del test	Prescrizione DEMA
Prerequisiti	FUN02_SIO_PS03 con esito Positivo
Input	Cliccare sul bottone "Impegnativa"
Output atteso	Apertura, in SSO, del modulo E-prescription
ID UAT	INT04_SIO_CCA01
Nome del test	Piano di lavoro interni

Prerequisiti	FUN02_SIO con esito positivo
Input	Cliccare sul bottone “Ricerca Da Pianificare”
Output atteso	Apertura Piano di lavoro interni: disponibilità richieste OE
ID UAT	INT04_SIO_CCA02
Nome del test	Piano di lavoro esterni
Prerequisiti	FUN02_SIO con esito positivo
Input	Cliccare sul bottone “Ricerca”
Output atteso	Apertura Piano di lavoro esterni: disponibilità richieste CUP
ID UAT	INT04_SIO_CCA03
Nome del test	Prescrizione DEMA
Prerequisiti	FUN02_SIO_CCA03 con esito Positivo
Input	Cliccare sul bottone “Impegnativa”
Output atteso	Apertura, in SSO, del modulo E-prescription
ID UAT	INT04_SIO_CCA04
Nome del test	Invio RSA a FSE
Prerequisiti	FUN02_SIO_CCA04 con esito Positivo
Input	Validazione RSA
Output atteso	Generazione documento e trasmissione a FSE
ID UAT	INT04_SIO_CCA05
Nome del test	Invio Certificato INPS
Prerequisiti	FUN02_SIO_CCA05 con esito Positivo
Input	Trasmissione Certificato
Output atteso	Ricevuta INPS: n. protocollo
ID UAT	INT04_SIO_SOWEB01
Nome del test	Trasmissione Diagnosi e Interventi
Prerequisiti	FUN02_SIO_SOWEB05 con esito Positivo
Input	Chiusura Atto Operatorio
Output atteso	Arrivo Diagnosi e Interventi su ADT nelle sezioni, rispettivamente “Diagnosi da Blocco Operatorio” e “Interventi da Blocco Operatorio”
ID UAT	INT04_SIO_SOWEB02
Nome del test	Scarico Materiali e Protesi
Prerequisiti	FUN02_SIO_SOWEB06 con esito Positivo
Input	Chiusura Atto Operatorio
Output atteso	Scarico Materiali e Protesi con successo
ID UAT	INT04_SIO_SOWEB03
Nome del test	Carico Prodotti e Farmaci (Integ. Con SOFIA – attiva solo in Arnas Brotzu)
Prerequisiti	FUN02_SIO_SOWEB03 con esito Positivo

Input	Inserimento Prodotti e Farmaci su SOFIA + Apertura Atto Operatorio
Output atteso	Acquisizione Prodotti e Farmaci da parte di Soweb

Tabella 342 - Test list piattaforma applicativa SISaR

La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.

7 CUTOVER - GOLDEN GATE E POWERED-ON

7.1 Pre-cutover

Questa fase anticipa una serie di attività propedeutiche per la fase finale, sempre allo scopo di ridurre al minimo il downtime.

Pertanto, è possibile eseguire le seguenti operazioni:

- Database¹:
 - Start cattura delle modifiche sul DB sorgente con GG;
 - Backup full + archive log del DB sorgente (RMAN);
 - Restore e recover iniziali ad un SCN XXX sul DB target (RMAN);
 - Apertura DB target e conversione in PDB;
 - Start replica delle modifiche catturate con GG, dall'SCN XXX+1 in poi sul DB target.
- Virtual machines:
 - Predisposizione sito VMware di transito.
 - Installazione vCenter Converter Standalone.
 - Test di conversione VM da Hyper-V a VMware.
 - Installazione e configurazione VMware Cloud Director Availability sul sito di transito.
 - Test migrazione VM da sito di transito, tramite VCDA, sull'ambiente target.
 - Predisposizione e configurazione DNS sull'ambiente target
 - Conversione VM e trasferimento nel sito di transito.
 - Configurare la migrazione utilizzando VMware Cloud Director Availability.
 - Avvio migrazione (5-6 gg prima del cutover).
 - 1° run test funzionali full.

¹ La RU del DB in essere sull'ambiente on-premise 19.3 non è supportata dal PSN. Pertanto, nell'ambiente target sarà eseguito un upgrade della RU ad una versione 19.22 sulla quale verranno eseguiti gli opportuni test per escludere problematiche di compatibilità.



Attività da svolgere in prossimità della fase di cutover.

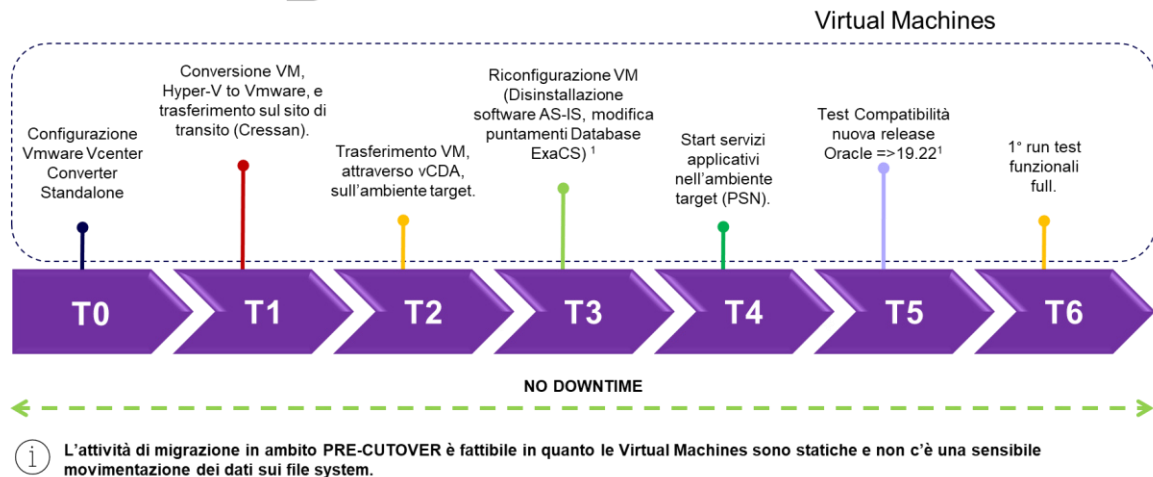


Figura 21 - Timeline Pre-cutover - Virtual Machines

Timeless	Task	Stima tempi	Note	ARES	ARES/ SardegnaIT	ARES/ Fornitore	PSN/TIM	PSN/ACN	PSN/ Dedalus	PSN/LDO
T0	Configurazione VMware Vcenter Converter Standalone	N/A	NO DOWNTIME	A	R	I	A	C	C	I
T1	Conversione VM, Hyper-V to VMware, e trasferimento sul sito di transito (Cressan).	N/A		A	R	C	A	C	C	I
T2	Trasferimento VM, attraverso vCDA, sull'ambiente target.	N/A		I	R	C	A	R	C	I
T3	Riconfigurazione VM (Disinstallazione software AS-IS, modifica puntamenti Database ExaCS)	N/A		I	I	C	A	C	R	I

T4	Start servizi applicativi nell'ambiente target (PSN).	N/A		I	I	R	A	C	R	I
T5	Test Compatibilità nuova release Oracle 19.22	N/A		I	I	C	A	C	R	I
T6	1° run test funzionali full.	2h		A/I	I	C	A	C	R	I

R: Responsible A: Accountable C: Consulted I: Informed

Tabella 343 - Task pre-cutover e matrice RACI

La fattibilità di questo scenario sarà confermata non appena si avrà l'ambiente (sito di transito «CRESSAN») e lo strumento disponibile per eseguire un test case reale.

7.2 Cutover

Per la fase di Cutover sono state individuate le seguenti operazioni:

Database:

Stop e inversione replica;

Virtual machines:

Stop applicativi.

Start applicativi.

2° run test funzionali (solo PSW 30 min).

DNS:

Switch DNS.

Nella seguente figura è riportata la timeline della fase di cutover:

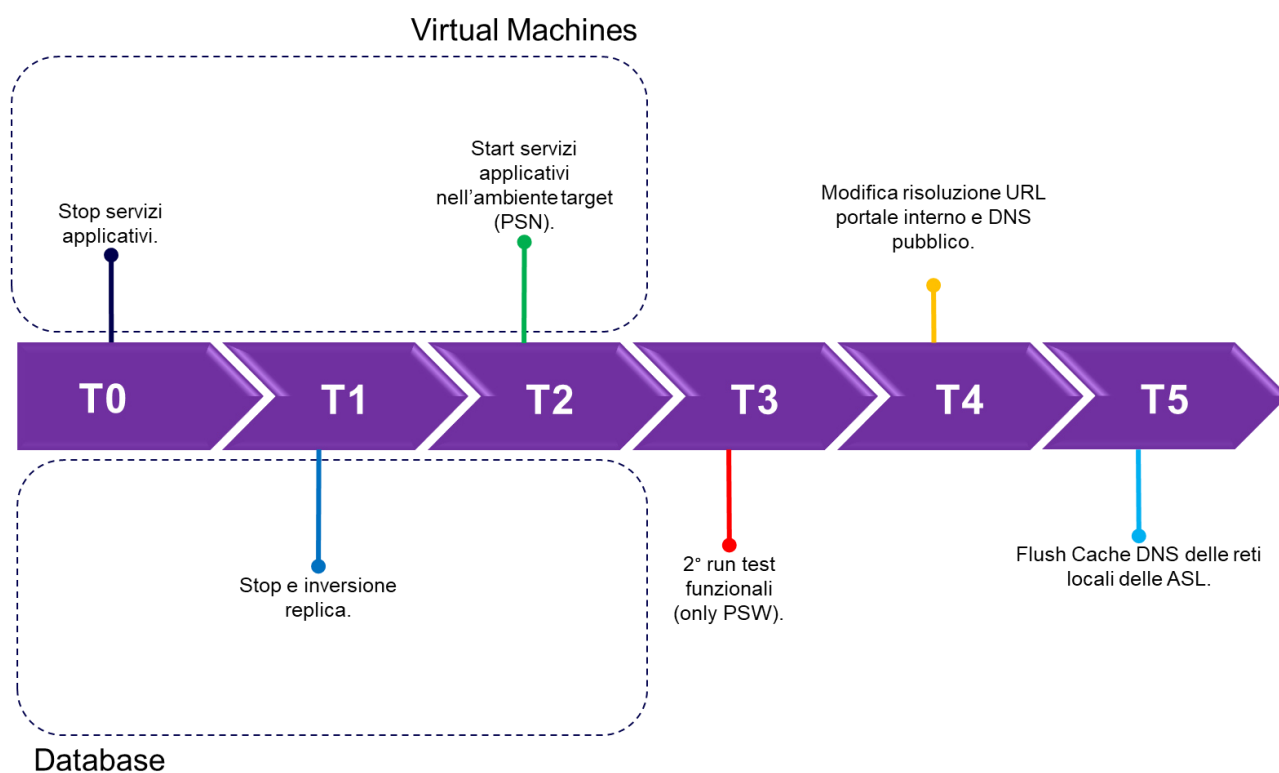


Figura 22 - Timeline cutover

Timeless	Database	Virtual Machine	Stima tempi	Note	ARES	ARES/ SardegnaIT	ARES/ Fornitore	PSN/TIM	PSN/ACN	PSN/ Dedalus	PSN/LDO
T0	-	Stop servizi applicativi.	15 min	Inserire pagina di cortesia per comunicare l'attività e relativo downtime.	A	I	R	A	C	R	I
T1	Stop e inversione replica.	-	20 min	-	A	I	R	A	R	C	I

T2	-	Start servizi applicativi nell'ambiente target (PSN).	15 min	Disattivare pagina di cortesia.	I	I	R	A	C	R	I
T3	2° run test funzionali (only PSW).		30 min	-	I	I	R	A	C	R	I
T4	Modifica risoluzione URL portale interno (il servizio PUA Comuni va su DNS pubblico).		30 min	-	A	R	C	A	I	C	I
T5	Flush Cache DNS delle reti locali delle ASL		30min	-	A	I	C	I	I	R	I

R: Responsible A: Accountable C: Consulted I: Informed

Tabella 344 - Dettaglio timeline di cutover

Per consentire il trasferimento dei dati relativi al tenant di produzione occorrerà prevedere le seguenti attività:

- Concordare le date con il cliente per il cutover applicativo;
- Comunicazione agli utilizzatori del sistema AS-IS da parte dell'ente dello stop delle attività in produzione a partire dalla data concordata;
- Spostamento dei dati come già indicato nel paragrafo 5.3;
- Attivazione del sistema in produzione nel nuovo tenant PSN;
- Rimappatura degli FQDN sul nuovo IP del tenant PSN con conseguente aggiornamento dei DNS pubblici (dove previsto).

8 ORGANIZZAZIONE

La struttura organizzativa generale lato PSN, nonché la descrizione delle competenze delle varie figure, sono specificate al paragrafo 5.1.1.2 del documento di Piano di Migrazione di Dettaglio.

Con riferimento a tale organizzazione, le figure di coordinamento e di interfaccia verso l'Amministrazione coinvolte nell'ambito della migrazione dei servizi SiSar sono le seguenti:

Ruolo	Nominativo	E-mail	Telefono
PMCA - Project Manager Contratto Attuativo	Federico Ferretti	federico.ferretti@telecomitalia.it	3356330270
Technical Team Leader (TTL)	Renato Rosicarelli	renato.rosicarelli@ext.noovle.com	3404647424
Project Manager (PM) TIM	Schirru Roberto	roberto.schirru@telecomitalia.it	3356330270
Project Manager (PM) Leonardo	Lombardelli Maurizio	maurizio.lombardelli@leonardo.com	3356330270

Tabella 345 - Referenti PSN per la Gestione della Migrazione del Servizio

Tali figure saranno supportate dalle strutture tecniche interne di TIM e Leonardo nonché dei partner coinvolti (c.d. PSN Enabler) che nel caso specifico sono:

- Accenture: ha competenza per la parte della progettazione di dettaglio della componente infrastrutturale nonché della sua configurazione;
- Dedalus: ha competenza per il supporto applicativo alla migrazione del parco applicativo SiSar. In particolare: supporto al team di Migration per Quality Assurance sui dati migrati, test applicativo (funzionali/prestazionali) sugli ambienti cloud PSN e supporto applicativo alle attività di switch off in produzione.

I riferimenti lato partner sono i seguenti:

PSN Enabler	Nominativo	E-mail	Telefono
Accenture	Igli Allushi	igli.allushi@accenture.com	349 4264884
Dedalus	Sandro Aresu	sandro.aresu@dedalus.com	340 2137380

Tabella 346 - Referenti PSN Enabler per la Gestione della Migrazione del Servizio

9 ANALISI RISCHI

Per quanto attiene ai rischi sulla sicurezza si faccia riferimento ai seguenti documenti, e relativi allegati, di Piano di Sicurezza, Piano di Qualità, Piano di Continuità Operativa, Manuale tecnico sulle misure di sicurezza “MTMS” reperibili in versione aggiornata al link <https://www.polostrategiconazionale.it/obiettivo-cloud/documentazione/>, nonché alle attività in corso di Vulnerability Assessment e Info Gathering e relativi esiti e remediation.

10 MONITORAGGIO

Monitoring Infrastrutturale

Come specificato al capitolo 5.3 del Progetto del Piano dei Fabbisogni, il PSN rende disponibile all’Amministrazione una piattaforma di gestione degli ambienti cloud unica (Console Unica).

All'interno della Console Unica vi è la sezione di “*Area Management & Monitoring*” che consente ai referenti delle Amministrazioni Contraenti di accedere alle funzionalità dedicate alla gestione e al monitoraggio delle risorse per ciascun servizio contrattualizzato e attivo all'interno delle specifiche piattaforme Cloud che erogano i servizi verticali.

Punto focale della soluzione è la componente di Event Detection, che ha come obiettivo l'analisi dei log e degli eventi generati dalle piattaforme Cloud che erogano i servizi verticali per tutte le attività svolte dall'Amministrazione; tale modulo, in particolare, verificherà la compliance di tutte le richieste effettuate rispetto al perimetro contrattuale e bloccherà eventuali attività che esulino da tale contesto inviando alert, anche tramite e-mail, sia ai referenti della PA abilitati all'utilizzo della CU sia agli operatori delle strutture di Operations preposte alla gestione delle segnalazioni di anomalia sui servizi erogati.

Monitoring applicativo

Relativamente al sistema SISAR si prevede il monitoraggio dei file di log applicativi, che sono costantemente monitorati da DEDALUS nelle normali attività di manutenzione.

All'interno dei moduli SISaR sono presenti diversi report di monitoraggio applicativo che possono essere utilizzati in modo manuale per:

- Monitorare il volume di dati prodotti, con una vasta copertura in quasi tutte le aree dei sistemi dipartimentali;
- Monitorare gli accessi utente.

Inoltre, è presente una soluzione di monitoraggio automatico basata su piattaforma Zabbix, che rileva situazioni anomale nelle code di integrazione, tra questi:

- Allineamento dati tra SISaR SIO e Trasfusionale;
- Allineamento dati tra SISaR SIO e Sistema LIS;
- Allineamento dati tra SISaR SIO e Sistema RIS;
- Allineamento dati tra SISaR SIO e Sistema Anatomia Patologica;
- Allineamento dati tra SISaR SIO e Sistema 118;
- Allineamento dati tra SISaR SIO e INAIL;
- Allineamento anagrafico tra SISaR dipartimentale e centralizzato;

La maggior parte di questi allarmi sono rilevati anche dai sistemi di monitoraggio dell'ESB Picasso.

Monitoring di Sicurezza

Nell'ambito dei servizi di sicurezza contrattualizzati è previsto quello di Security Event Monitoring, Notification & Log Management, il quale è erogato remotamente tramite il Centro Servizi Leonardo di Chieti, che effettua attività di monitoraggio continuativo per mezzo di un SOC presidiato H24 per 365 giorni l'anno e composto da un gruppo di specialisti (analisti, system engineer, security tester e malware specialist).

Il servizio utilizza la piattaforma di Security Information and Event Management (SIEM) e, grazie a sistemi di indicizzazione e correlazione evoluti, fornisce il monitoraggio continuo degli eventi di sicurezza generati dalle

componenti di sicurezza previste nel perimetro di gestione del Secure Device Management. Il servizio è progettato per identificare rapidamente risorse o eventi potenzialmente dannosi, anticipando tempestivamente i potenziali attacchi informatici o tentativi di attacco. Il servizio, erogato in modalità H7x24 e si articola nelle seguenti fasi:

- Onboarding/Startup: è la fase che precede l'avvio del servizio vero e proprio, con la presa in carico degli accessi alle piattaforme deputate alla "Detection", l'analisi degli allarmi configurati sulle stesse;
- Monitoraggio degli eventi: costante controllo degli allarmi scaturiti dalla correlazione degli eventi di sicurezza raccolti;
- Identificazione: a seguito della ricezione di un allarme generato dalle piattaforme previste dalla presente proposta o direttamente dall'Organizzazione tramite segnalazione, il SOC genera opportuno ticket sulla piattaforma di trouble ticketing;
- Classificazione: il SOC effettua l'analisi di primo livello per escludere falsi positivi e per classificare in base alle informazioni in proprio possesso il livello di criticità dell'incidente in esame (Triage);
- Analisi e Notifica: il SOC completa l'analisi dell'incidente avviando il servizio di incident notification per mezzo del ticket che conterrà tutte le informazioni raccolte e le indicazioni di eventuali azioni di contenimento come descritto nel successivo paragrafo;
- Tuning: fase di supporto operativo verso i gestori delle piattaforme tecnologiche deputate alla "Detection" attivata nel caso di tuning necessario sulle stesse per limitare o azzerare l'incidenza di falsi positivi e del conseguente "rumore" da essi generato; Il servizio di TRIAGE (identification, classification, notification) ha l'obiettivo di facilitare la messa a punto dei falsi positivi e di segnalare all'Amministrazione le anomalie reali. Il processo di Incident Notification ha come obiettivo la rapida e corretta comunicazione agli attori interessati. Il processo alla base è lo standard previsto dall'incident management per le comunicazioni e le escalation. A tale proposito, nel corso della fase di avvio del servizio saranno identificate le opportune interfacce competenti per la ricezione delle notifiche in funzione della classe degli asset coinvolti e della criticità dell'incidente;
- Continuous Improvement: Le attività sono finalizzate ad eseguire un tuning specifico sulle piattaforme contenute nel perimetro di interesse del servizio. Le attività di Continuous Improvement consentono nel tempo un evidente beneficio, migliorando la risposta dei sistemi di Security Event Monitoring a fronte dell'insorgere di nuove minacce, consentendo una maggiore coerenza delle politiche di sicurezza implementate e nel rispetto delle modalità organizzative adottate dall'Amministrazione. Il servizio di monitoraggio è stato dimensionato in modo specifico per ogni ente, in base al perimetro infrastrutturale indicato nel Piano e oggetto di migrazione.

ALLEAGATO 1 – ARCHITETTURA DI NETWORKING E SICUREZZA

Il presente allegato ha lo scopo di illustrare l'architettura generale di networking e sicurezza dell'infrastruttura PSN contrattualizzata da ARES, al fine di fornire una visione complessiva del progetto all'interno del quale sono collegati i tenant afferenti al progetto "SiSar". Per semplicità di lettura, il presente allegato non riporta i dettagli sul tenant e reti afferenti al progetto AREUS.

L'architettura prevede, sotto una stessa Organizzazione rappresentata da ARES, la realizzazione di un Tenant dedicato a ciascuna delle 12 Aziende Sanitarie nonché di un Tenant dedicato ai servizi centralizzati oggi afferenti al CRESSAN (DC H-Cloud presso il sito di Regione Sardegna di Cagliari – via Posada). Tale architettura avrà pertanto una struttura multi-tenant, come di seguito rappresentato.

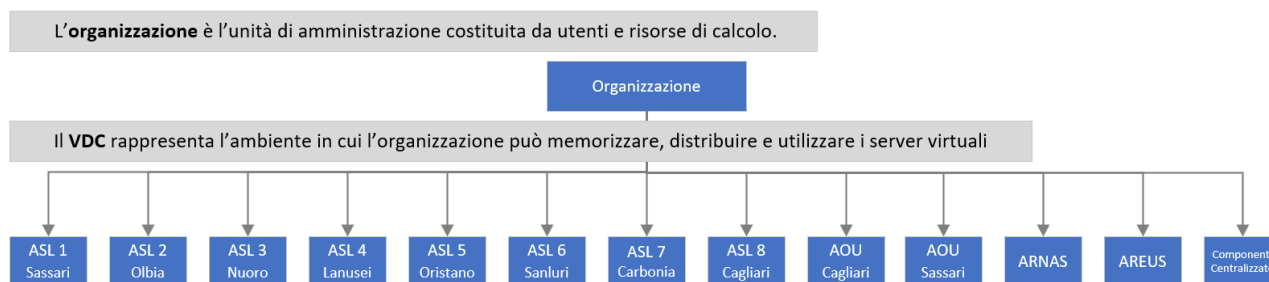


Figura 1 - Architettura Multi Tenant

Inoltre, l'architettura è completata con i servizi PaaS DB previsti da progetto erogati sulla infrastruttura Industry Standard (MS SQL) o PSN Managed (Oracle).

In particolare, mentre per il primo caso la raggiungibilità è interna alla infrastruttura Industry Standard mediante stringa di connessione, per il DB Oracle sarà necessario aprire due porte (a garanzia di alta affidabilità) FastConnect a 10G verso l'infrastruttura PSN Managed Oracle del DC PSN (c.d. DRCC - Dedicated Region - Cloud@Customer) di Acilia ove risiedono gli apparati ExaCS sui quali verrà istanziato il servizio.

RETE DI INTERCONNESSIONE VERSO / DA PSN

L'architettura proposta è progettata per gestire una unica connettività MPLS a 10 Gbps dedicata al progetto da condividersi tra tutti i Tenant, mentre per il traffico verso Internet si utilizzerà la banda condivisa resa disponibile dai DC PSN.

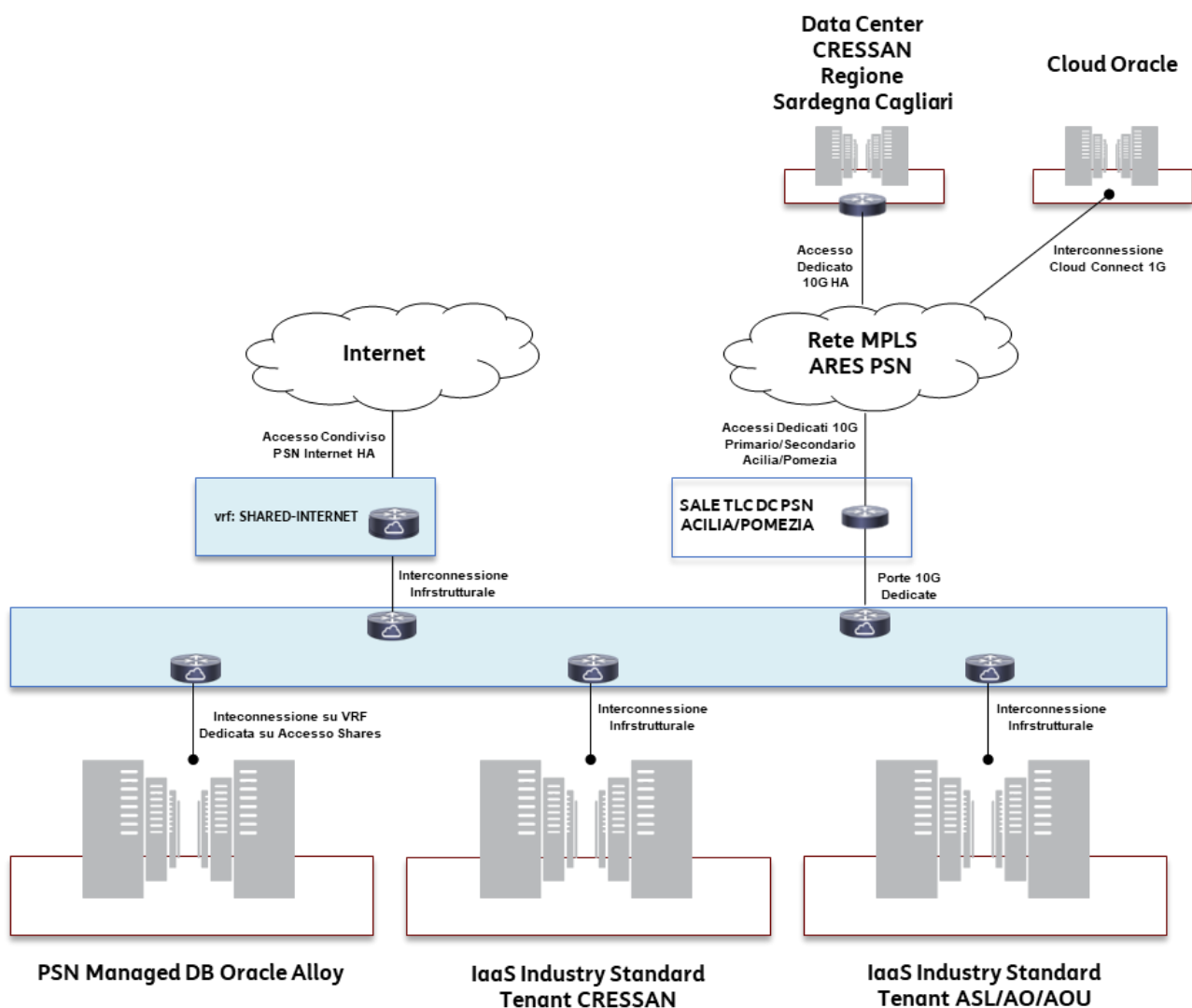
Nel caso specifico la connettività dedicata è funzionale alla erogazione dei servizi anche nella fase di esercizio a regime in quanto la tipologia di dati "critici" gestiti e veicolati dalle applicazioni necessita di racchiudere il traffico all'interno di VPN, quali quelle MPLS, aventi il massimo grado di protezione nei confronti del mondo esterno.

Sui diversi collegamenti MPLS è associata una rete di transito dietro la quale vengono annunciate le subnet IP relative alle sedi Cliente o ai Tenant PSN.

A tale scopo l'Amministrazione ha assegnato al progetto le seguenti subnet dalle quali attingere senza rischi di sovrapposizioni con quelle attualmente in uso sulla RTR:

- Rete MPLS 10G Generale: 172.25.3.224/29, 172.25.3.232/29, 172.25.3.240/29, 172.25.3.248/29.

La figura successiva schematizza la rete poc'anzi descritta e della quale, nel seguito, si forniscono ulteriori dettagli.



RETE 10G MPLS CONDIVISA TRA I TENANT

- I due collegamenti terminati presso i due DC PSN di Acilia e Pomezia sono realizzati in Affidabilità Standard (singolo accesso e singolo apparato di terminazione OADM + router) ma sono configurati uno in backup all'altro a livello L3 sfruttando l'interconnessione L2 in essere tra i due DC PSN, assimilabili ad un unico Data virtuale.

Ciascun collegamento è interconnesso alla Fabric ACI del DC PSN di terminazione ed entrambi saranno visti da un virtual router PSN. I due router di terminazione dei collegamenti condividono il proprio stato mediante il protocollo di Internal BGP, mentre tra gli stessi ed il virtual router PSN viene utilizzato il protocollo di External BGP. Nella configurazione implementata il collegamento di Acilia sarà considerato come primario mentre quello di Pomezia come backup.

Per entrambe le tipologie di collegamento è presente una rete di transito dietro la quale sono annunciate le subnet IP delle sedi Cliente o dei Tenant PSN. In particolare, sono in utilizzo le due subnet 172.25.3.224/29 e 172.25.3.232/29/29 come meglio dettagliato nel successivo paragrafo.

Modalità di Terminazione dei Collegamenti

Lato DC CRESSAN i collegamenti, ed i relativi apparati (terminazione OADM Slim e router), sono terminati all'interno di appositi spazi rack resi disponibili dall'Amministrazione.

Presso i due DC PSN di Acilia e Pomezia è invece prevista da progetto PSN:

- L'housing della terminazione di rete OADM Slim e del router presso appositi spazi rack individuati nella sala TLC dei due DC PSN;
- Il cablaggio passivo in fibra ottica per la realizzazione del rilancio tra la sala TLC e la porta dell'apparato ACI di attestazione della connessione alla Infrastruttura PSN;
- La predisposizione della porta a 10G dell'apparato ACI di attestazione della connessione alla Infrastruttura PSN.
- La configurazione interna del networking sulla infrastruttura PSN per consentire la raggiungibilità dei Tenant dalla rete MPLS ARES.

Si evidenzia che ciascun Tenant sarà raggiungibile attraverso le subnet IP ad esso assegnato secondo la ripartizione presente in Tabella 6 – Piano di Indirizzamento IP dei Tenant PSN.

Piano di Indirizzamento IP Reti di Transito

Per il collegamento in Affidabilità Elevata presso il DC CRESSAN si rende necessario utilizzare una intera /29 tra quelle assegnate. La tabella seguente ne dettaglia l'impiego.

Sede	Servizio	Network IP Transito	Netmask	IP Ethernet Router	IP VRRP Router	IP Apparati CRESSAN
Data Center Regione Sardegna - Via Posada, 1 – 09122 Cagliari (CA)	Accesso Primario MPLS 10G - Sede Master VRF ARES	172.25.3.224	255.255.255.248	172.25.3.226	172.25.3.225	I tre IP residui saranno disponibili per l'assegnazione agli apparati lato LAN della rete di transito
	Accesso Backup MPLS 10G - Sede Master VRF ARES			172.25.3.227		

Tabella 1 – Piano di Indirizzamento IP Rete di Transito Collegamento 10G HA DC RAS CRESSAN

Per i collegamenti presso i DC PSN di Acilia e Pomezia si rende necessario utilizzare una intera /29 tra quelle assegnate. La tabella seguente ne dettaglia l'impiego.

Sede	Servizio	Network IP Transito	Netmask	IP Ethernet Router	IP e-BGP	IP Ethernet Fabric ACI
DC PSN Acilia (Sala TLC) - Via Di Macchia Palocco, 223 – 00125 Roma (RM)	Accesso Primario MPLS 10G - Sede Slave VRF ARES	172.25.3.232	255.255.255.248	172.25.3.233	172.25.3.236	172.25.3.237
DC TIM PSN Pomezia (Sala TLC) - Via Pontina, Km 29 – 00040 Pomezia (RM)	Accesso Backup MPLS 10G - Sede Slave VRF ARES			172.25.3.234		172.25.3.238

Tabella 2 – Piano di Indirizzamento Rete IP di Transito Collegamenti 10G DC PSN Acilia e Pomezia

INTERCONNESSIONE DB ORACLE DRCC

L'architettura proposta, corredata delle varie tipologie di interconnessione possibili verso l'infrastruttura DB, è illustrata nella successiva Figura 3 - Architettura di Interconnessione Oracle DRCC.

Di fatto, mediante l'apertura delle porte FastConnect dedicate interne alla infrastruttura PSN collegate alla fabric, la connettività verso DRCC viene inserita nella stessa VRF già prevista per la connettività esterna. I casi di interconnessione possibili verso il DB Oracle sono i seguenti:

- Oracle DRCC può essere esposto su Global Internet;
- Oracle DRCC può essere esposto su MPLS;
- Oracle DRCC colloquia con lo IaaS.

Tale ventaglio di possibilità rende la soluzione flessibile anche nell'ottica delle strategie di migrazione che possono essere adottate.

Per entrambe la raggiungibilità del DB su Oracle DRCC sono state assegnate le due classi di indirizzamento IP Privato 172.25.4.192/27 e 172.25.4.160/27 il cui dettaglio di utilizzo sarà specificato in un documento dedicato alla progettazione del DRCC-EXACS.

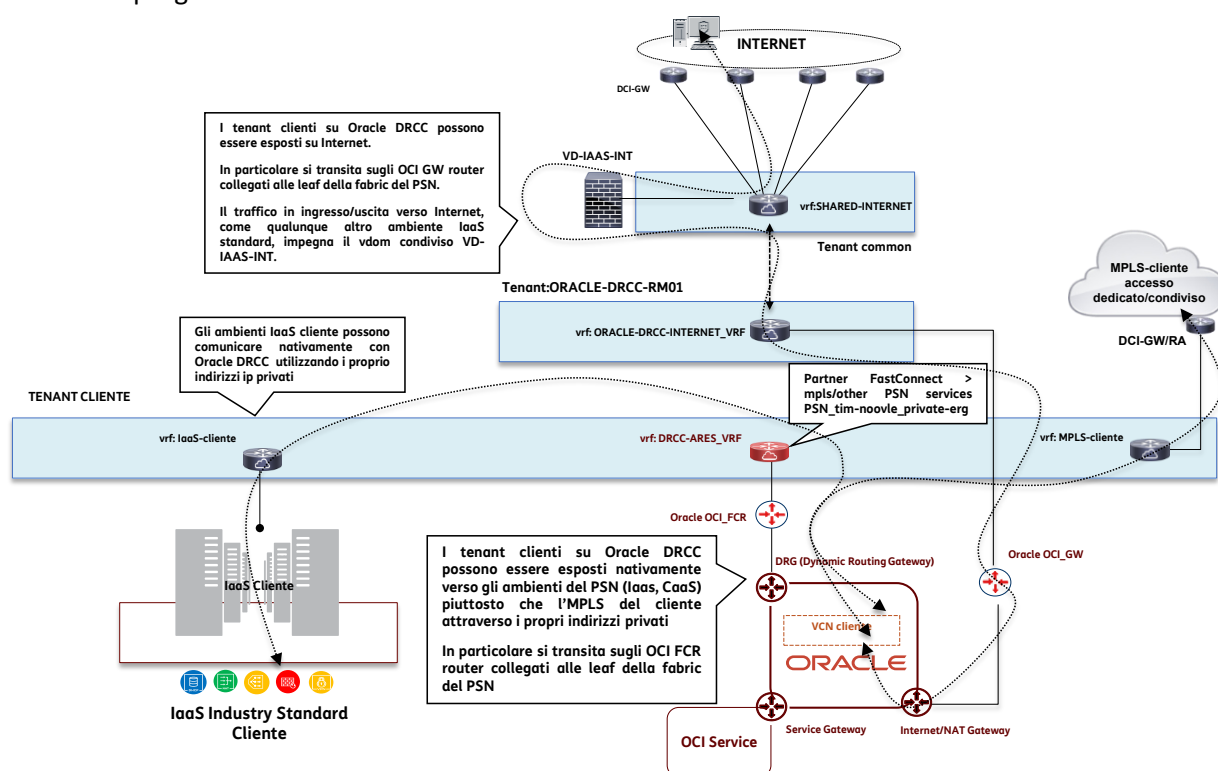


Figura 3 - Architettura di Interconnessione Oracle DRCC

SICUREZZA DEI TENANT

Per quanto attiene agli aspetti di sicurezza, ciascun Tenant dispone di propri dispositivi virtuali (vNGFW, vWAF, etc.) necessari ad erogare i servizi di protezione previsti dal progetto.

In particolare, sono previste due distinte architetture di sicurezza, la prima per il Tenant CRESSAN deputato alla erogazione dei servizi centralizzati e la seconda per i 12 Tenant afferenti alle altrettante Aziende Sanitarie.

In linea generale l'architettura sarà costituita da più layer logici, i quali verranno consolidati in maniera definitiva in fase di implementazione, anche alla luce delle risultanze delle attività di Cyber Security Assessment precedentemente descritte.

L'architettura logica di protezione del Tenant CRESSAN è rappresentata graficamente nella figura successiva.

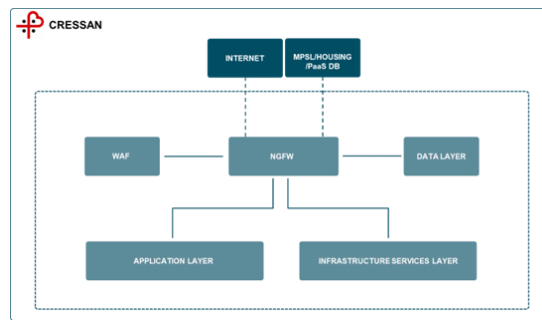


Figura 4 - Architettura Logica di Sicurezza Tenant CRESSAN

Nello specifico, l'NGFW a perimetro dell'infrastruttura garantirà la segregazione e la segmentazione dei vari layer logici, ispezionando sia il traffico intra-tenant che quello destinato alle reti untrusted.

In tale infrastruttura è previsto un WAF (Web Application Firewall) per l'analisi e la protezione del traffico HTTP e HTTPS, proteggendo in maniera mirata attacchi su risorse WEB, quali ad esempio: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, XML Injection e altre vulnerabilità definite da OWASP (Open Web Application Security Project).

L'architettura logica di protezione dei 12 Tenant afferenti alle Aziende Sanitarie è altresì rappresentata graficamente nella figura successiva.

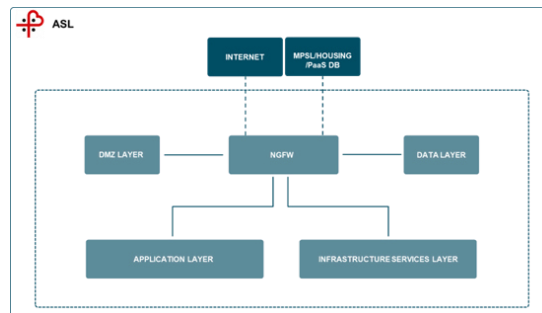


Figura 5 - Architettura Logica di Sicurezza Tenant Aziende Sanitarie

A differenza del Tenant di CRESSAN, nei N.12 Tenant sarà assente il WAF.

Di seguito, vengono riportati i principi generali considerati nel processo di definizione dell'architettura di sicurezza:

- Segmentazione della rete e configurazione in HA delle macchine:
L'architettura di sicurezza atta a proteggere la piattaforma applicativa oggetto del presente documento è composta dai seguenti elementi:
 - NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;
 - WAF: Web Application Firewall per la mitigazione di eventuali attacchi di natura applicativa (L7). Tale strumento gestirà il traffico in ingresso dalle reti Untrusted, come ad esempio Internet, e potrà anche essere utilizzato per l'esposizione di portali/web application interne;
 - EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

La segregazione delle sottoreti è stata definita in base ai livelli applicativi, distinguendo Presentation, Application e Data layer, allo scopo di isolare i vari server, sulla base del livello di criticità ed esposizione a minacce di sicurezza, riducendo così la superficie di attacco.

Sia i Firewall sia i WAF saranno configurati in alta affidabilità sfruttando le funzionalità insite, rispettivamente, sul FortiOS 7.0.15 e FortiADC 7.4.3. Relativamente ai Firewall, In caso di fault della macchina principale, il tempo di attivazione del nodo passivo è inferiore a 1s. Relativamente ai WAF la tempistica è dipendente da numerosi parametri (frequenza e numero di heartbeat, ARP, etc.) ed il cui valore ottimale è in corso di definizione con il vendor Fortinet.

- Sistema di Firewalling:

Di default i firewall saranno configurati con delle policy di tipo deny all, consentendo il solo traffico specificamente autorizzato e indicato nei documenti di Progetto Esecutivo di Dettaglio relativi ai singoli servizi in migrazione. Sulle macchine sarà abilitato il profilo IPS/IDS nei confronti di tutti i flussi da/verso le reti untrusted (es. Internet). La scelta di abilitare la modalità in sola detection (IDS), piuttosto che quella in prevention (IPS), scaturisce a seguito di un'attenta analisi del comportamento della componente applicativa, in quanto l'IPS potrebbe influire sulla corretta erogazione del servizio applicativo, data la sua natura proattiva.

- Sistema WAF:

Il sistema WAF è orientato all'analisi ed alla protezione del traffico HTTP e HTTPS, proteggendo in maniera mirata attacchi su risorse WEB, quali ad esempio: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, XML Injection e altre vulnerabilità definite da OWASP Top Ten (Open Web Application Security Project). L'aggiornamento delle signature avverrà in maniera automatica. Per ogni applicazione, oltre alle signature di default, saranno previste delle policy custom implementate in fase di learning mode.

- Crittografia dei dati in transito e gestione delle chiavi:

I NGFW/WAF utilizzano la crittografia SSL/TLS per HTTPS. Quando si stabilisce una connessione SSL/TLS, è possibile controllare il livello di crittografia e le suite di cifratura da utilizzare, al fine di controllare il livello di sicurezza dei dati in transito. Non verranno utilizzati protocolli deprecati. Allo stato attuale il Progetto del Piano dei Fabbisogni non ha previsto soluzioni centralizzate per la gestione e distribuzione delle chiavi di crittografia. Tali funzionalità possono essere implementate a seguito di analisi ad hoc e valutazione del relativo effort aggiuntivo.

- Wilcard SSL

La fornitura dei certificati SSL rientra nell'ambito delle competenze dell'Amministrazione. Nei casi specifici sarà valutata e condivisa l'effettiva applicabilità degli stessi in base alle best practice di sicurezza.

- Gestione delle Identità e degli Accessi:

- MFA per accessi in VPN/Console di sicurezza;
- VPN Site-to-Site con FortiAuthenticator con il SOC LDO;
- Per gli accessi alla Console Unica di PSN è rilasciata la funzionalità di accesso MFA.

Allo stato attuale il Progetto del Piano dei Fabbisogni non ha previsto l'utilizzo di sistemi PAM. Tale funzionalità può essere implementata a seguito di analisi ad hoc e valutazione del relativo effort aggiuntivo.

- Monitoraggio degli eventi e KPI:

Il dettaglio delle attività di monitoraggio degli eventi è riportato nel paragrafo 5.5.2.3 Security Event Monitoring, Notification & Log Management del Progetto del Piano dei Fabbisogni approvato dall'Amministrazione. I KPI previsti per l'erogazione di tale servizio sono riportati nella successiva tabella.

KPI		SLA
KPI #1	Time to take in charge Alert (since Alert creation)	15 minutes for the 90% of the high severity cases
		4 hours for the 100% of the cases
KPI #2	Alert classification and notification (starting from KPI #1)	30 minutes for the 90% of the cases
		4 hours for the 100% of the cases

Tabella 3 – KPI Security Event Monitoring, Notification & Log Management

- Management:

L'ambiente che si propone è caratterizzato da una rete di management in cui risiederanno le console di gestione e i cruscotti delle piattaforme di security.

La configurazione delle VM atte alla protezione dei singoli Tenant è riportata nelle successive tabelle, la prima delle quali riferita al Tenant CRESSAN e la seconda ai 12 Tenant delle Aziende Sanitarie.

# VM	Ruolo	CPU Totale [#]	RAM Totale [GB]	Storage Encrypted Totale [GB]	OS e versione
1	NGFW1 (Tipo VM04V)	4	16	250	OVA
2	NGFW2 (Tipo VM04V)	4	16	250	OVA
3	NGFW3 (Tipo VM04V)	4	16	250	OVA
4	NGFW4 (Tipo VM04V)	4	16	250	OVA
5	WAF1	4	12	250	OVA
6	WAF2	4	12	250	OVA
7	WAF3	4	12	250	OVA
8	WAF4	4	12	250	OVA
9	SIEM (Log collector / forwarder)	4	8	200	OVA
10	Scan Engine	4	4	200	OVA
11	Management	4	4	100	OVA

Tabella 4 – Configurazione VM di Sicurezza Tenant CRESSAN

# VM	Ruolo	CPU Totale [#]	RAM Totale [GB]	Storage Encrypted Totale [GB]	OS e versione
1	NGFW1 (Tipo VM04V)	4	16	250	OVA
2	NGFW2 (Tipo VM04V)	4	16	250	OVA
3	SIEM (Log collector / forwarder)	4	4	200	OVA
4	Scan Engine	4	4	200	OVA
5	Management	4	4	100	OVA

Tabella 5 – Configurazione VM di Sicurezza Tenant ASL / AO / AOU

Considerate le specificità dei singoli servizi, le specifiche configurazioni di sicurezza (es. crittografia nei flussi) saranno contenute all'interno dei relativi Progetti Esecutivi di Dettaglio.

Architettura High Level Tenant CRESSAN

L'architettura High Level di sicurezza del Tenant CRESSAN è di seguito schematizzata.

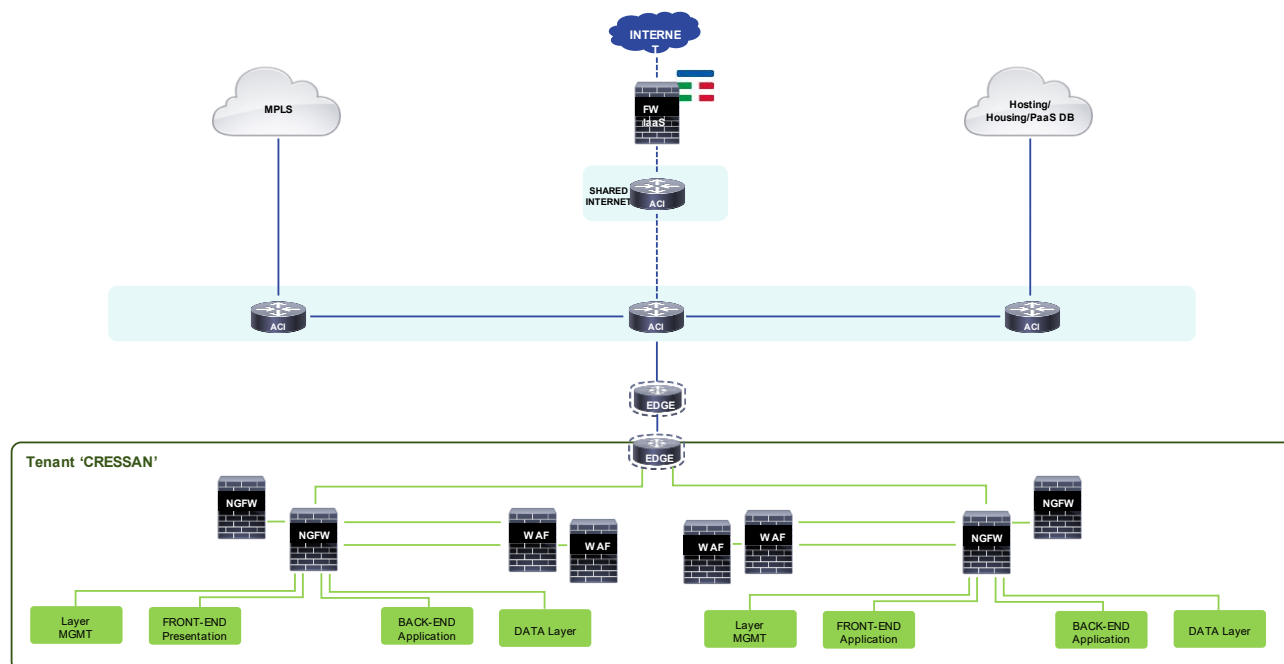


Figura 6 - Architettura High level di Sicurezza Tenant CRESSAN

Tale architettura è composta dai seguenti elementi:

- NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS, Web Filtering, Security DNS, Explicit Proxy, Application Control;
- WAF: Web Application Firewall per la mitigazione di eventuali attacchi di natura applicativa (L7);
- EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.
- Il Tenant ospiterà anche le virtual appliance per la scansione delle vulnerabilità (Virtual Scan Engine) ed il Log Collector per la raccolta degli eventi di sicurezza da inoltrare verso il SOC.

E' stato scelto di utilizzare due coppie di NGFW in alta affidabilità (in configurazione attivo-passivo) per superare dei vincoli infrastrutturali introdotti dall'architettura Industry Standard mono-tenant in cui ogni virtual appliance può avere al massimo 10 interfacce.

Questo vincolo comunque è stato sfruttato per dare maggiore flessibilità orizzontale alla distribuzione dei sistemi e può permettere un ulteriore livello di affidabilità fornito dalla presenza di 2 nodi NGFW.

La distribuzione degli applicativi dietro i 2 nodi firewall verrà definita in base al traffico e alle necessità elaborative richieste.

La segregazione delle sottoreti è stata scelta in base ai livelli applicativi, distinguendo Presentation, Application e Data layer.

Il profilo IPS/IDS dell'NGFW verrà implementato su tutti i flussi da/verso le reti untrusted (es. Internet). La scelta di abilitare la modalità in sola detection (IDS), piuttosto che quella in prevention (IPS), scaturisce a seguito di un'attenta analisi del comportamento della componente applicativa in quanto l'IPS potrebbe influire sulla corretta erogazione del servizio applicativo data la sua natura proattiva.

Il WAF è lo strumento che gestisce il traffico in ingresso dalle reti Untrusted come ad esempio Internet.

Lo stesso potrà essere utilizzato anche per l'esposizione di portali/web application interne. Anche in questo caso la configurazione è in alta affidabilità (attivo-passivo).

Architettura High Level Tenant Aziende Sanitarie

L'architettura high level di sicurezza dei tenant delle Aziende Sanitarie è di seguito schematizzata.

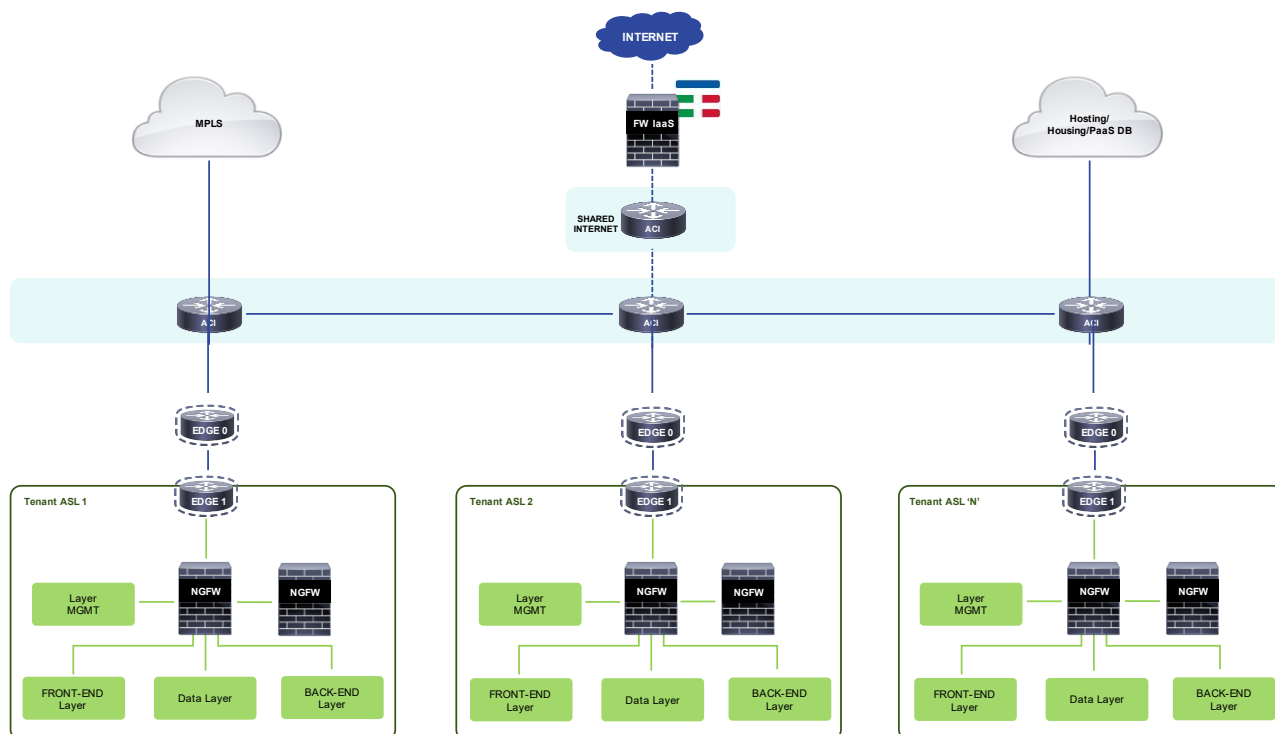


Figura 7 - Architettura High level di Sicurezza Tenant Aziende Sanitarie

Tale architettura è composta dai seguenti elementi:

- NGFW: Next generation Firewall (L7) con funzionalità di IPS/IDS , Web Filtering, Security DNS, Explicit Proxy, Application Control;
- EDGE: Gateway Edge vCloud Director con funzionalità di FW distribuito (L3/L4) con la possibilità di utilizzare i security tag per la micro-segmentazione/segregazione.

L'architettura è caratterizzata dalle seguenti peculiarità:

- Comunicazione Infra-Tenant: Avverrà attraverso i VRF (Virtual Routing and Forwarding) e se necessario attraverso delle VPN Site-to-Site;
- Esposizioni Cressan: I flussi applicativi verranno gestiti, controllati ed ispezionati dal WAF, per tutti gli altri flussi si utilizzerà NGFW.
- Esposizione Servizi: In fase di assessment e raccolta dati sull'AS-IS, non sono emerse esposizioni di web application/portali dalle singole entità periferiche.

Eventuali esposizioni di altra natura verranno gestite, controllate ed ispezionate dal NGFW del singolo tenant.

Nel caso in cui si volesse esporre un portale presente su uno dei Tenant delle ASL, il traffico verrebbe ri-direzionato verso il Tenant CRESSAN, ispezionato dal WAF e re-inoltrato verso il Tenant di destinazione.

Definizione dei Fabbisogni Inerenti i Piani di Indirizzamento IP

La scelta del Piano d'Indirizzamento è basato su due criteri: l'utilizzo di 4096 IP resi disponibili dall'Amministrazione con la classe 10.77.0.0/20 e la massima ottimizzazione della numerosità per ciascuna subnet in base alle attuali effettive necessità.

Tenant CRESSAN

Il fabbisogno calcolato per il tenant CRESSAN prevede l'impiego di:

- N° 4 subnet /24;
- N° 2 subnet /25;
- N° 4 subnet /26;
- N° 4 subnet /27.

Da utilizzarsi come da schema successivo.

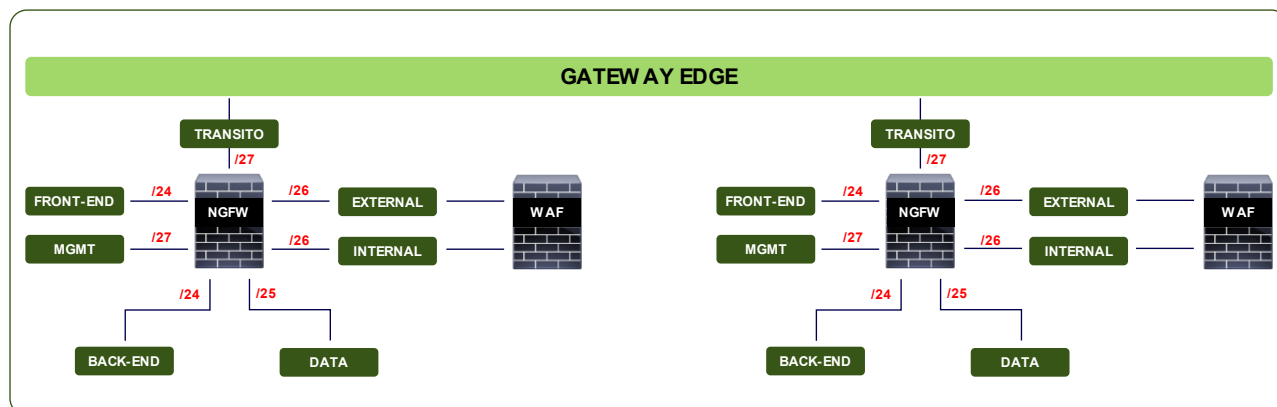


Figura 8 – Utilizzo Subnet Tenant CRESSAN

Tenant ASL / AOU / ARNAS

Il fabbisogno calcolato per i tenant ASL / AOU / ARNAS prevede l'impiego di N° 5 subnet /27 da utilizzarsi come da schema successivo.

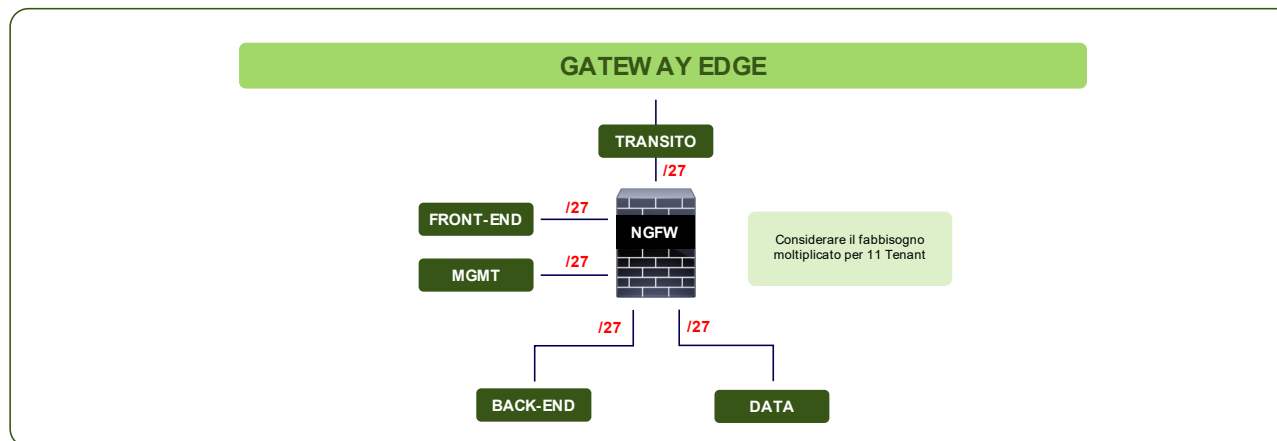


Figura 9 – Utilizzo Subnet Tenant ASL / AOU / ARNAS

Flussi di Traffico

In questo paragrafo si riportano i flussi di comunicazioni tra i vari Tenant IaaS e le reti Trusted ed Untrusted ad essi afferenti.

Flussi – Inbound da Rete Internet

Di seguito si riporta un esempio di flusso Inbound da rete Internet verso un Web Server ospitato nel Front-End Layer del Tenant CRESSAN.

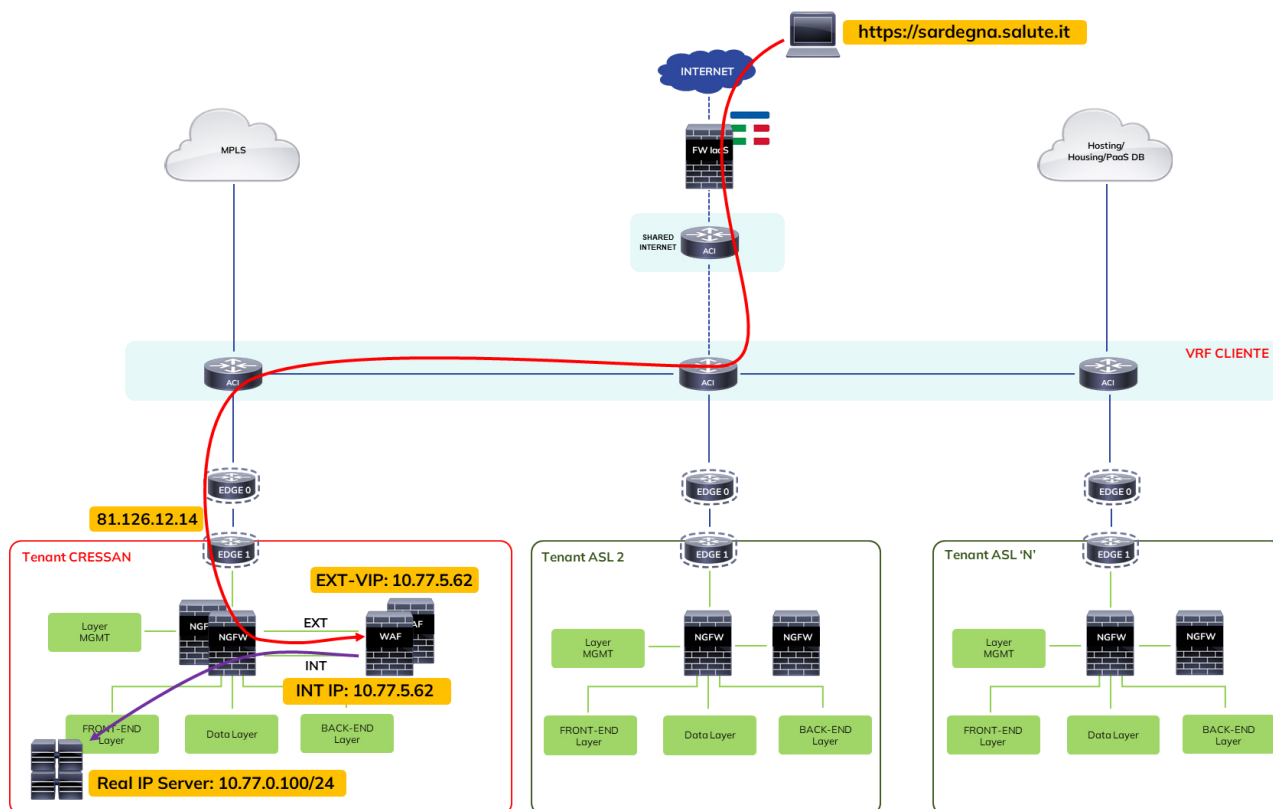


Figura 10 - Esempio di flusso inbound Tenant CRESSAN

Come possibile osservare in Figura 10 si ha il seguente scenario:

1. Un Utente effettua una richiesta <https://sardegna.salute.it> da rete Internet;
2. La richiesta viene inoltrata dopo opportuna risoluzione DNS verso l'indirizzo pubblico del Tenant CRESSAN;
3. Viene Effettuato un primo DNAT con Relativa Policy Firewall (Gateway EDGE) verso un Virtual IP appartenente al WAF su interfaccia External. (81.126.12.14 DNAT -> 10.77.5.62);
4. La richiesta verrà analizzata e quindi ispezionata dal WAF. Se verrà ritenuta lecita verrà re-inoltrata verso il Real Server attraverso l'interfaccia Internal del WAF, viceversa sarà bloccata o segnalata in base alla configurazione adottata sul WAF;
5. La richiesta arriverà al Real Server presente nel Front-End Layer.

Si sottolinea che per poter ispezionare il traffico sarà necessario importare il certificato SSL dei vari Real Server che espongono i diversi servizi nel Web Application Firewall.

Flussi – Inbound da Rete MPLS

Di seguito si riporta un esempio di flusso Inbound da rete MPLS verso un Web Server ospitato nel Front-End Layer del Tenant CRESSAN.

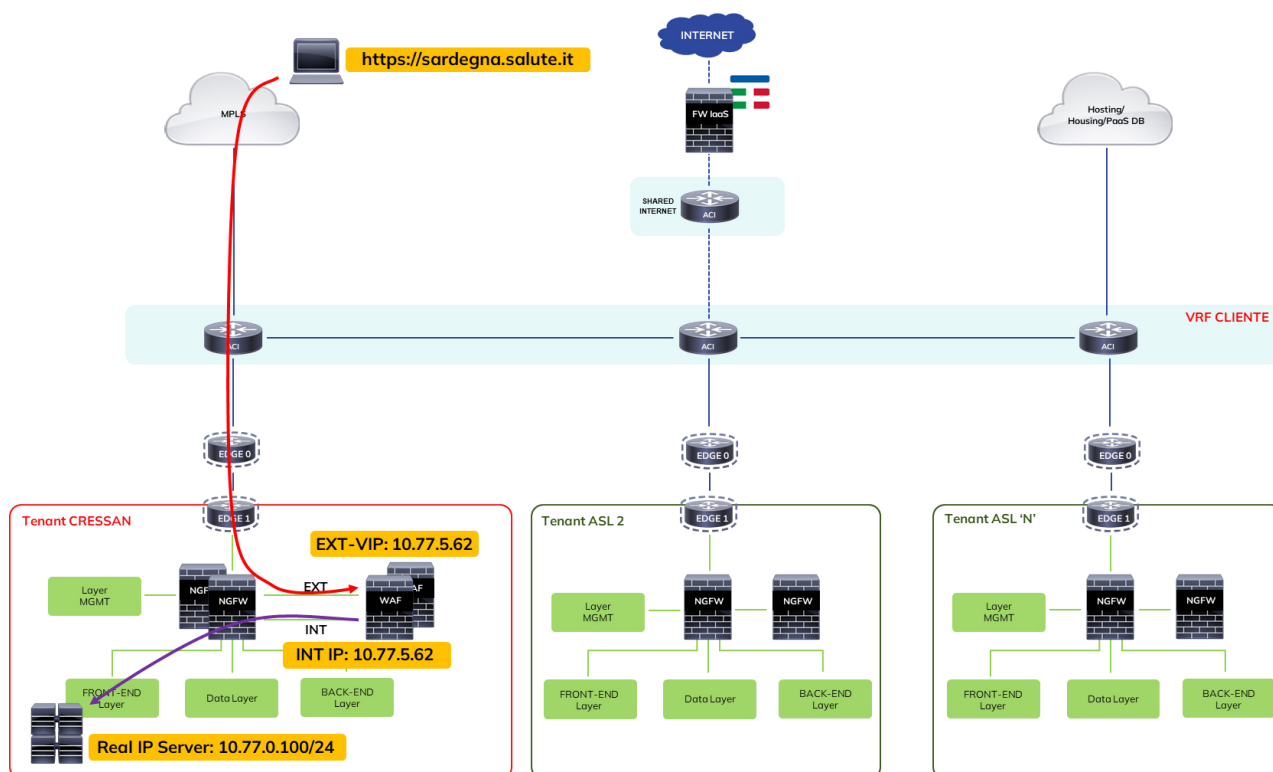


Figura 11 - Flusso Inbound da rete MPLS vs Tenant CRESSAN

Come possibile osservare in Figura 11 si ha il seguente scenario:

1. Un Utente effettua una richiesta `https://sardegna.salute.it` da rete MPLS;
2. La richiesta viene inoltrata dopo opportuna risoluzione DNS verso il WAF attraverso il Gateway EDGE;
3. La richiesta verrà analizzata e quindi ispezionata dal WAF. Se verrà ritenuta lecita verrà re-inoltrata verso il Real Server attraverso l'interfaccia Internal del WAF, viceversa sarà bloccata o segnalata in base alla configurazione adottata sul WAF;
4. La richiesta arriverà al Real Server presente nel Front-End Layer.

Si sottolinea che per poter ispezionare il traffico sarà necessario importare il certificato SSL dei vari Real Server che espongono i diversi servizi nel Web Application Firewall.

Inoltre, si potrà re-inoltrare la richiesta verso il real server anche in SSL-Off Loading (Traffico non Cifrato).

Flussi – Inbound da Rete MPLS vs Tenant ASL 1

Di seguito si riporta un esempio di flusso Inbound da rete MPLS verso un Web Server ospitato nel Front-End Layer del Tenant CRESSAN.

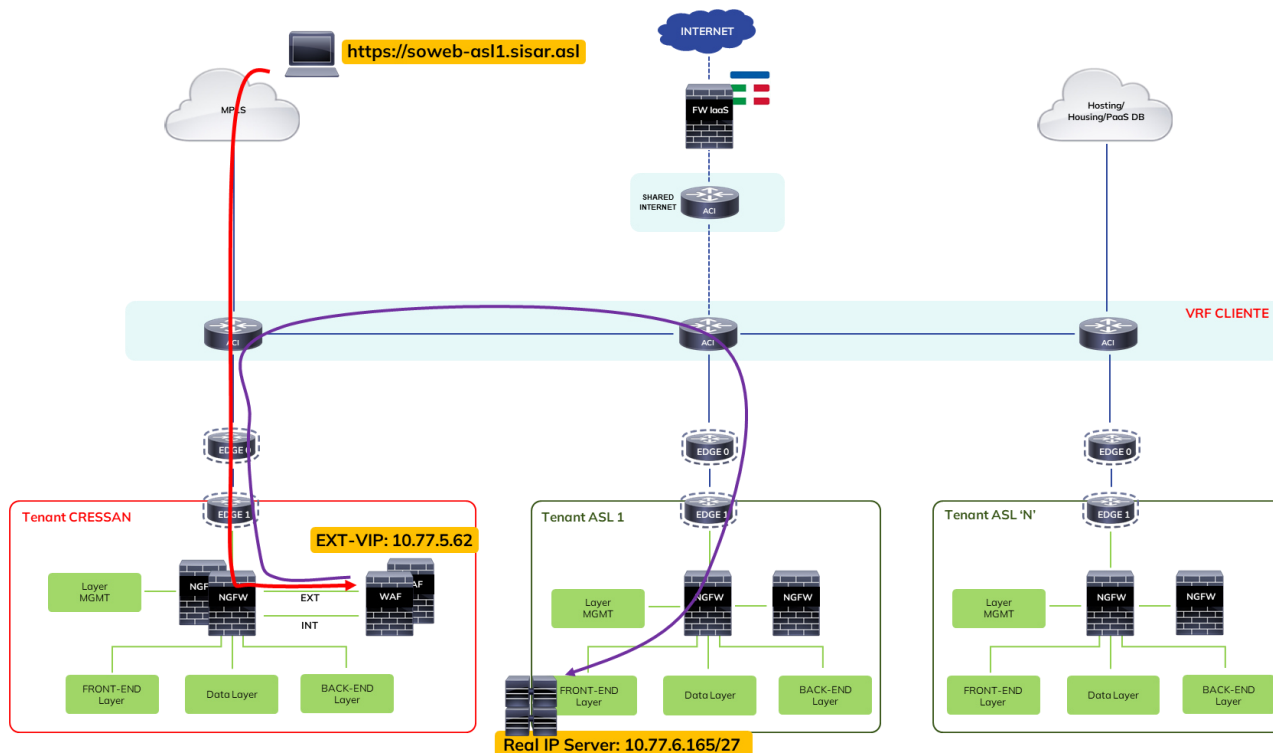


Figura 12 - Flusso Inbound da rete MPLS vs Tenant ASL 1

Come possibile osservare in Figura 12 si ha il seguente scenario:

1. Un Utente effettua una richiesta `https://soweb-asl1.sisar.asl` da rete MPLS;
2. La richiesta viene inoltrata dopo opportuna risoluzione DNS verso il WAF attraverso il Gateway EDGE;
3. La richiesta verrà analizzata e quindi ispezionata dal WAF. Se verrà ritenuta lecita verrà re-inoltrata verso il Real Server (ospitato nel Tenant ASL1) attraverso l'interfaccia External del WAF, viceversa sarà bloccata o segnalata in base alla configurazione implementata sul WAF;
4. La richiesta arriverà al Real Server presente nel Front-End Layer del Tenant ASL1 per mezzo della VRF Cliente che consente l'interconnessione tra i Tenant.

I flussi Inbound provenienti da reti Untrusted, verso il WAF, verranno sottoposti a terminazione SSL/TLS, caratterizzata dalla decifratura del traffico crittografato, con successiva ispezione, utile ad individuare potenziali minacce cyber. Dopo l'ispezione, il WAF può ri-crittografare il traffico prima di inviarlo all'applicazione. Questo processo non solo migliora la sicurezza, ma può anche offrire benefici prestazionali, poiché il terminatore di sessione può liberare le risorse del server di back-end dall'onerosa operazione di decifratura (SSL Offloading).

Il traffico verrà quindi ispezionato al fine di identificare e proteggere l'infrastruttura da attacchi su risorse WEB, quali ad esempio: Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), SQL Injection, XML Injection e altre vulnerabilità definite da OWASP (Open Web Application Security Project). Il WAF può proteggere le applicazioni con controlli dell'accesso basati sui dati di geo-localizzazione, sulla lista di inclusione e sugli indirizzi IP in blacklist, sull'URL HTTP (Hypertext Transfer Protocol Uniform Resource Locator) e sull'intestazione HTTP.

Inoltre, tale appliance di sicurezza intercetta tutte le richieste indirizzate ai server di back-end (es. Application Layer) occultando i dettagli degli stessi mascherando, ad esempio, il loro indirizzo IP, la configurazione e altri dettagli che potrebbero essere sfruttati da un attore malevolo al fine di condurre un attacco.

Si sottolinea che per poter ispezionare il traffico sarà necessario importare il certificato SSL dei vari Real Server che espongono i diversi servizi nel Web Application Firewall.

Inoltre, si potrà re-inoltrare la richiesta verso il real server anche in SSL-Off Loading (Traffico non Cifrato).

Nel caso in cui non sarà necessario l'utilizzo del WAF si potrà indirizzare il traffico dall'MPLS direttamente al Tenant che ospita il servizio richiesto e controllare ed ispezionare tali flussi attraverso il NGFW di perimetro del relativo Tenant.

Flussi – Tenant CRESSAN e Tenant ASL 2

Di seguito si riporta un esempio di flusso tra il Tenant CRESSAN ed il Tenant ASL 2. L'interconnessione tra i TENANT avviene per mezzo delle VRF (Virtual Routing and Forwarding).

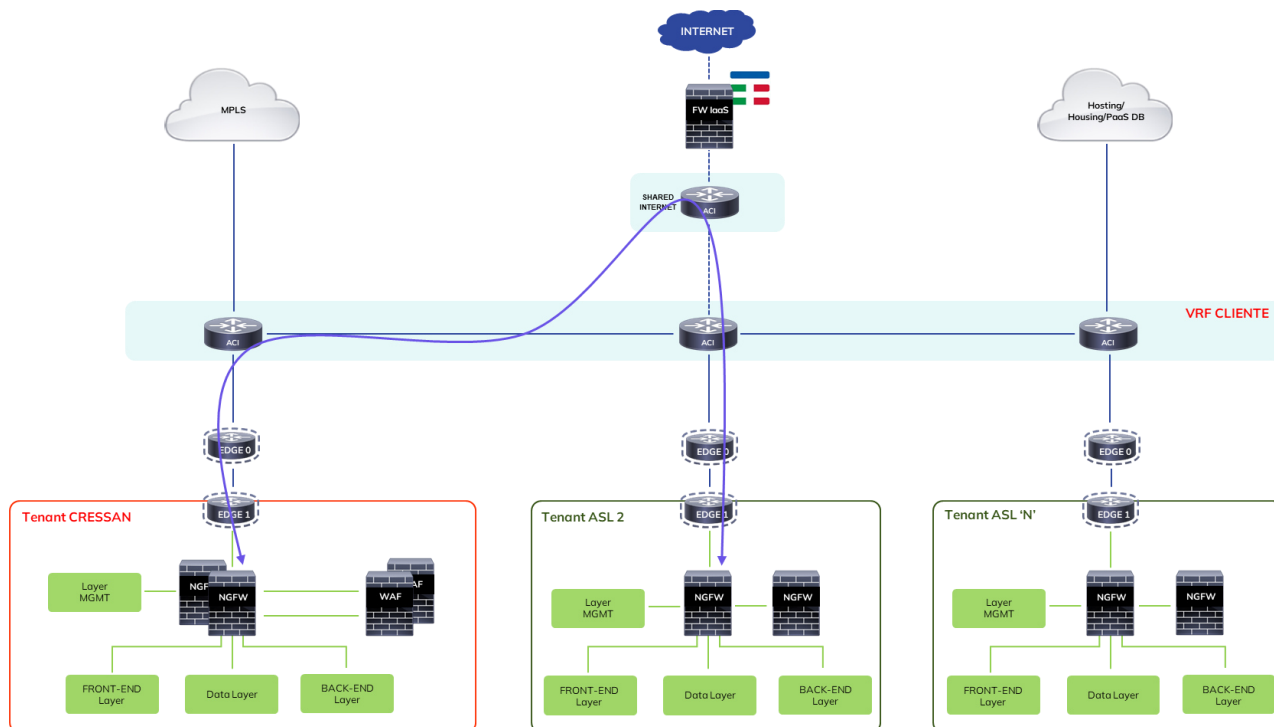


Figura 13 – Flusso di comunicazione tra due TENANT

In tal caso il traffico verrà controllato ed ispezionato per mezzo dei firewall di perimetro dei relativi Tenant.

Flussi – Tenant CRESSAN e PaaS DB

Di seguito si riporta un esempio di flusso tra il Tenant CRESSAN ed il Tenant PaaS DB. L'interconnessione tra i TENANT avviene per mezzo delle VRF (Virtual Routing and Forwarding).

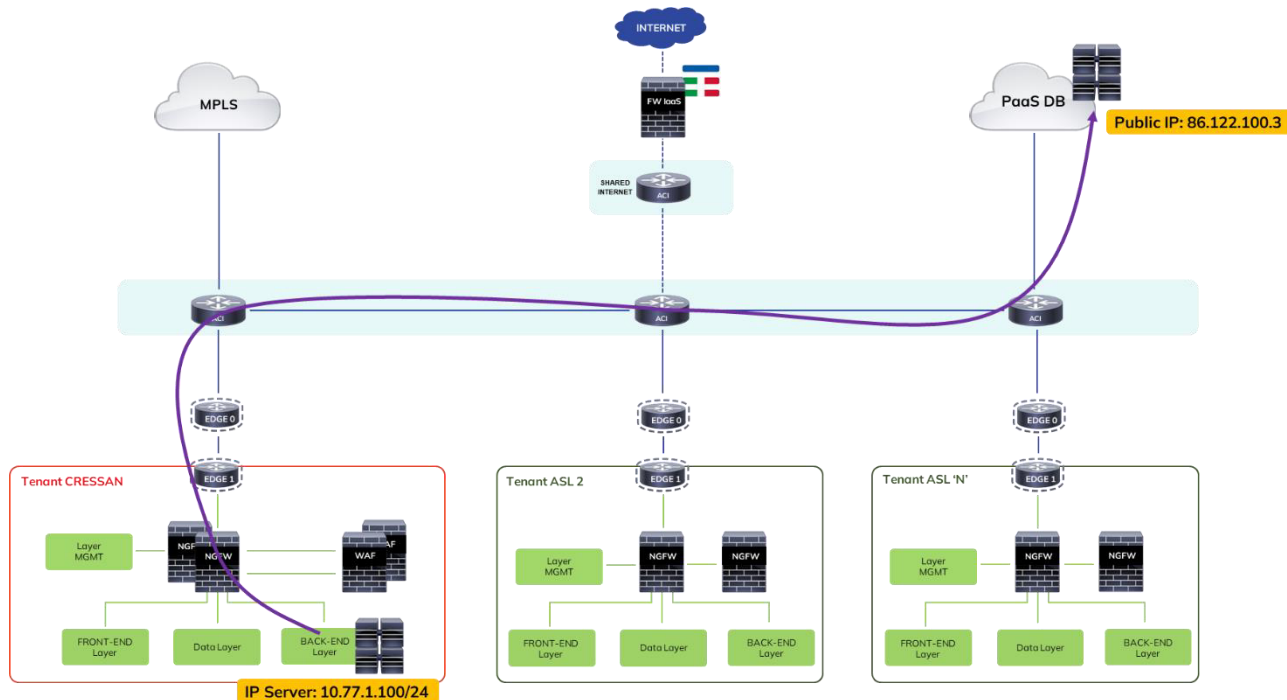


Figura 14 - Flusso tra Tenant IaaS e Tenant PaaS DB

Per ciò che concerne tali flussi verranno controllati ed ispezionati dai vari firewall di perimetro del singolo Tenant.

Come possibile osservare in figura 14 verranno implementate delle policy Firewall puntuali.

Flussi – Outbound tra Tenant CRESSAN ed Internet

Di seguito si riporta un esempio di flusso Outbound dal Tenant CRESSAN verso Internet.

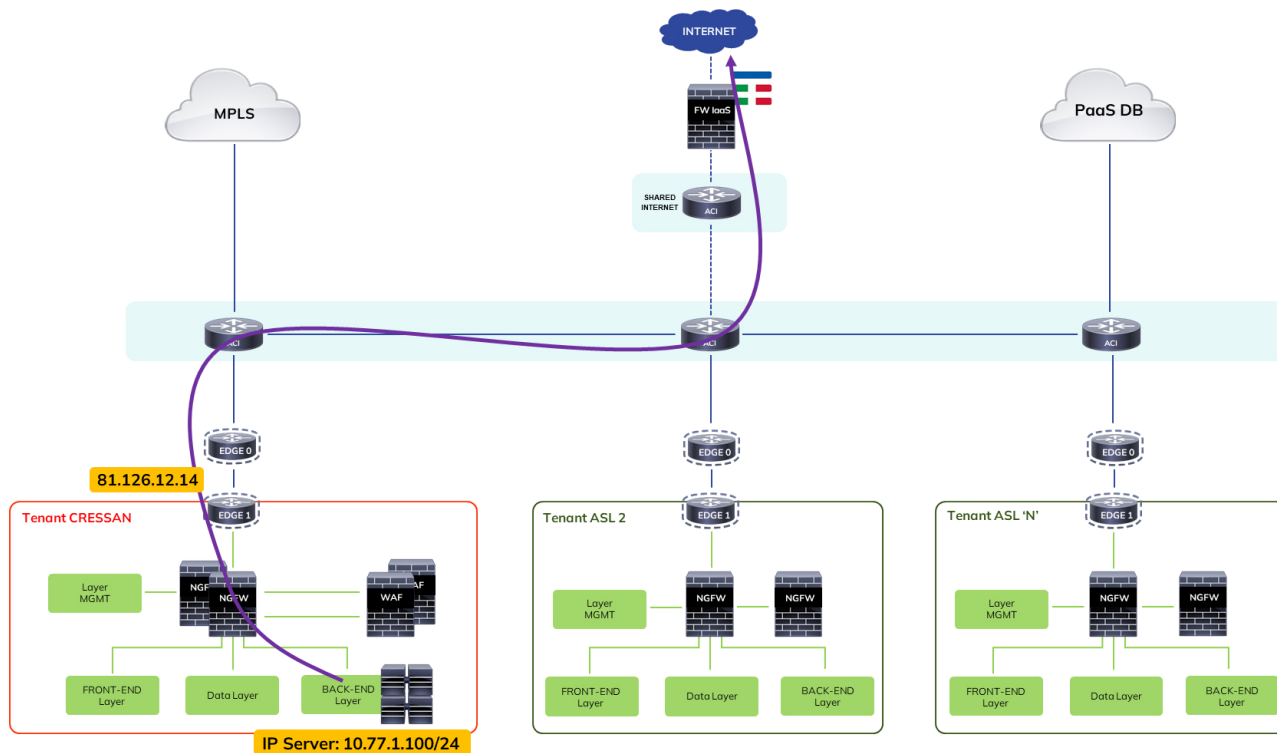


Figura 15 – Flussi di traffico tra Tenant CRESSAN e Internet

Come possibile osservare in Figura 15 il traffico in outbound verso Internet viene controllato ed ispezionato attraverso il NGFW di perimetro del Tenant CRESSAN.

In tali apparati sarà possibile configurare le funzionalità di sicurezza quali ad esempio: Web Filtering, IPS/IDS, DNS Security, Proxy esplicito.

PIANO DI INDIRIZZAMENTO IP INTERNO DEI TENANT

TENANT	Layer	NGFW	CIDR	Subnet Address	Host Address Range
CRESSAN	FRONT-END	1	/24	10.77.0.0/24	10.77.0.1 - 10.77.0.254
CRESSAN	BACK-END	1	/24	10.77.1.0/24	10.77.1.1 - 10.77.1.254
CRESSAN	FRONT-END	2	/24	10.77.2.0/24	10.77.2.1 - 10.77.2.254
CRESSAN	BACK-END	2	/24	10.77.3.0/24	10.77.3.1 - 10.77.3.254
CRESSAN	DATA	1	/25	10.77.4.0/25	10.77.4.1 - 10.77.4.126
CRESSAN	DATA	2	/25	10.77.4.128/25	10.77.4.129 - 10.77.4.254
CRESSAN	EXTERNAL WAF	1	/26	10.77.5.0/26	10.77.5.1 - 10.77.5.62
CRESSAN	INTERNAL WAF	1	/26	10.77.5.64/26	10.77.5.65 - 10.77.5.126
CRESSAN	EXTERNAL WAF	2	/26	10.77.5.128/26	10.77.5.129 - 10.77.5.190
CRESSAN	INTERNAL WAF	2	/26	10.77.5.192/26	10.77.5.193 - 10.77.5.254
CRESSAN	TRANSITO	1	/27	10.77.6.0/27	10.77.6.1 - 10.77.6.30
CRESSAN	MGMT	1	/27	10.77.6.32/27	10.77.6.33 - 10.77.6.62
CRESSAN	TRANSITO	2	/27	10.77.6.64/27	10.77.6.65 - 10.77.6.94
CRESSAN	MGMT	2	/27	10.77.6.96/27	10.77.6.97 - 10.77.6.126
ASL1 SASSARI	TRANSITO	N.A.	/27	10.77.6.128/27	10.77.6.129 - 10.77.6.158
ASL1 SASSARI	FRONT-END	N.A.	/27	10.77.6.160/27	10.77.6.161 - 10.77.6.190
ASL1 SASSARI	BACK-END	N.A.	/27	10.77.6.192/27	10.77.6.193 - 10.77.6.222
ASL1 SASSARI	DATA	N.A.	/27	10.77.6.224/27	10.77.6.225 - 10.77.6.254
ASL1 SASSARI	MGMT	N.A.	/27	10.77.7.0/27	10.77.7.1 - 10.77.7.30
ASL 2 OLBIA	TRANSITO	N.A.	/27	10.77.7.32/27	10.77.7.33 - 10.77.7.62
ASL 2 OLBIA	FRONT-END	N.A.	/27	10.77.7.64/27	10.77.7.65 - 10.77.7.94
ASL 2 OLBIA	BACK-END	N.A.	/27	10.77.7.96/27	10.77.7.97 - 10.77.7.126
ASL 2 OLBIA	DATA	N.A.	/27	10.77.7.128/27	10.77.7.129 - 10.77.7.158
ASL 2 OLBIA	MGMT	N.A.	/27	10.77.7.160/27	10.77.7.161 - 10.77.7.190
ASL 3 NUORO	TRANSITO	N.A.	/27	10.77.7.192/27	10.77.7.193 - 10.77.7.222
ASL 3 NUORO	FRONT-END	N.A.	/27	10.77.7.224/27	10.77.7.225 - 10.77.7.254
ASL 3 NUORO	BACK-END	N.A.	/27	10.77.8.0/27	10.77.8.1 - 10.77.8.30
ASL 3 NUORO	DATA	N.A.	/27	10.77.8.32/27	10.77.8.33 - 10.77.8.62
ASL 3 NUORO	MGMT	N.A.	/27	10.77.8.64/27	10.77.8.65 - 10.77.8.94
ASL 4 LANUSEI	TRANSITO	N.A.	/27	10.77.8.96/27	10.77.8.97 - 10.77.8.126
ASL 4 LANUSEI	FRONT-END	N.A.	/27	10.77.8.128/27	10.77.8.129 - 10.77.8.158
ASL 4 LANUSEI	BACK-END	N.A.	/27	10.77.8.160/27	10.77.8.161 - 10.77.8.190
ASL 4 LANUSEI	DATA	N.A.	/27	10.77.8.192/27	10.77.8.193 - 10.77.8.222
ASL 4 LANUSEI	MGMT	N.A.	/27	10.77.8.224/27	10.77.8.225 - 10.77.8.254
ASL 5 ORISTANO	TRANSITO	N.A.	/27	10.77.9.0/27	10.77.9.1 - 10.77.9.30
ASL 5 ORISTANO	FRONT-END	N.A.	/27	10.77.9.32/27	10.77.9.33 - 10.77.9.62

TENANT	Layer	NGFW	CIDR	Subnet Address	Host Address Range
ASL 5 ORISTANO	BACK-END	N.A.	/27	10.77.9.64/27	10.77.9.65 - 10.77.9.94
ASL 5 ORISTANO	DATA	N.A.	/27	10.77.9.96/27	10.77.9.97 - 10.77.9.126
ASL 5 ORISTANO	MGMT	N.A.	/27	10.77.9.128/27	10.77.9.129 - 10.77.9.158
ASL 6 SANLURI	TRANSITO	N.A.	/27	10.77.9.160/27	10.77.9.161 - 10.77.9.190
ASL 6 SANLURI	FRONT-END	N.A.	/27	10.77.9.192/27	10.77.9.193 - 10.77.9.222
ASL 6 SANLURI	BACK-END	N.A.	/27	10.77.9.224/27	10.77.9.225 - 10.77.9.254
ASL 6 SANLURI	DATA	N.A.	/27	10.77.10.0/27	10.77.10.1 - 10.77.10.30
ASL 6 SANLURI	MGMT	N.A.	/27	10.77.10.32/27	10.77.10.33 - 10.77.10.62
ASL 7 CARBONIA	TRANSITO	N.A.	/27	10.77.10.64/27	10.77.10.65 - 10.77.10.94
ASL 7 CARBONIA	FRONT-END	N.A.	/27	10.77.10.96/27	10.77.10.97 - 10.77.10.126
ASL 7 CARBONIA	BACK-END	N.A.	/27	10.77.10.128/27	10.77.10.129 - 10.77.10.158
ASL 7 CARBONIA	DATA	N.A.	/27	10.77.10.160/27	10.77.10.161 - 10.77.10.190
ASL 7 CARBONIA	MGMT	N.A.	/27	10.77.10.192/27	10.77.10.193 - 10.77.10.222
ASL 8 CAGLIARI	TRANSITO	N.A.	/27	10.77.10.224/27	10.77.10.225 - 10.77.10.254
ASL 8 CAGLIARI	FRONT-END	N.A.	/27	10.77.11.0/27	10.77.11.1 - 10.77.11.30
ASL 8 CAGLIARI	BACK-END	N.A.	/27	10.77.11.32/27	10.77.11.33 - 10.77.11.62
ASL 8 CAGLIARI	DATA	N.A.	/27	10.77.11.64/27	10.77.11.65 - 10.77.11.94
ASL 8 CAGLIARI	MGMT	N.A.	/27	10.77.11.96/27	10.77.11.97 - 10.77.11.126
AOU CAGLIARI	TRANSITO	N.A.	/27	10.77.11.128/27	10.77.11.129 - 10.77.11.158
AOU CAGLIARI	FRONT-END	N.A.	/27	10.77.11.160/27	10.77.11.161 - 10.77.11.190
AOU CAGLIARI	BACK-END	N.A.	/27	10.77.11.192/27	10.77.11.193 - 10.77.11.222
AOU CAGLIARI	DATA	N.A.	/27	10.77.11.224/27	10.77.11.225 - 10.77.11.254
AOU CAGLIARI	MGMT	N.A.	/27	10.77.12.0/27	10.77.12.1 - 10.77.12.30
AOU SASSARI	TRANSITO	N.A.	/27	10.77.12.32/27	10.77.12.33 - 10.77.12.62
AOU SASSARI	FRONT-END	N.A.	/27	10.77.12.64/27	10.77.12.65 - 10.77.12.94
AOU SASSARI	BACK-END	N.A.	/27	10.77.12.96/27	10.77.12.97 - 10.77.12.126
AOU SASSARI	DATA	N.A.	/27	10.77.12.128/27	10.77.12.129 - 10.77.12.158
AOU SASSARI	MGMT	N.A.	/27	10.77.12.160/27	10.77.12.161 - 10.77.12.190
ARNAS	TRANSITO	N.A.	/27	10.77.12.192/27	10.77.12.193 - 10.77.12.222
ARNAS	FRONT-END	N.A.	/27	10.77.12.224/27	10.77.12.225 - 10.77.12.254
ARNAS	BACK-END	N.A.	/27	10.77.13.0/27	10.77.13.1 - 10.77.13.30
ARNAS	DATA	N.A.	/27	10.77.13.32/27	10.77.13.33 - 10.77.13.62
ARNAS	MGMT	N.A.	/27	10.77.13.64/27	10.77.13.65 - 10.77.13.94

Tabella 6 – Piano di Indirizzamento IP dei Tenant PSN

Ares Sardegna - Azienda Regionale della Salute

PROGETTO ESECUTIVO DI DETTAGLIO

**SISTEMA INFORMATIVO SANITARIO INTEGRATO
REGIONALE (SISaR)**

ExaDB-D Provisioning Guidelines

Versione 1.1 – 29 maggio 2025

Elenco dei Contenuti

- Cronologia Delle Versioni 3
 - Revisori 3
 - Elenco delle Modifiche 3
- Scopo del Documento 4
- Acronimi 4
- Naming Convention 4
- Segregazione degli Ambienti 4
- Exadata Cloud Service Infrastructure 4
 - Configurazione..... 4
 - Configurazioni Mandatorie..... 5
 - Configurazioni per la Maintenance 5
 - Tagging..... 5
- Exadata Cloud Service VM Cluster..... 6
 - Networking 6
 - Custom DNS Resolution..... 6
 - Virtual Cloud Network 7
 - Client Subnets..... 7
 - Backup Subnets 7
 - Gateways 8
 - Security Lists e Routing Tables 8
 - Configurazione..... 9

Indice delle Figure

- Figura 1 - Networking Architecture 6

Cronologia Delle Versioni

Revisori

Nome	Versione	Data

Elenco delle Modifiche

Versione	Data Modifica	Modificato da	Tipo di Modifica

Scopo del Documento

Il presente documento fornisce linee guida dettagliate per il provisioning del servizio **Oracle Exadata Cloud Service on Dedicated Infrastructure** nella tenancy PSN di ARES, comprendendo informazioni relative alla predisposizione della configurazione di rete, dell'infrastruttura e dei VM Cluster relativi al servizio.

Acronimi

Naming Convention

Segregazione degli Ambienti

Per implementare la segregazione degli ambienti, non produttivi da quelli produttivi, verrà effettuato il provisioning dei Database in Oracle Home separate, individuate in un unico VM Cluster all'interno di una sola Oracle Exadata Cloud Service Infrastructure (sistema fisico), il provisioning dell'ExaDB-D infrastructure avverrà in un compartment dedicato.

In particolare, i compartments sono i seguenti:

Attributo	Ambito	Ambiente Comune
Compartment	ExaDB-D Infrastructure	cmp-exinfra
Compartment	Networking	cmp-network
Compartment	ExaDB-D VM Cluster	cmp-database

Oltre alla segregazione applicativa, basata su differenti Oracle Home, i Database verranno segregati mediante l'uso di diversi Container e Pluggable Database all'interno del VM Cluster.

Exadata Cloud Service Infrastructure

Per l'elenco completo dei passi per il provisioning di una Exadata Cloud Service Infrastructure fare riferimento alla documentazione ufficiale, consultabile alla URL: <https://docs.oracle.com/en-us/iaas/exadatacloud/doc/ecs-manage-infrastructure.html#ECSCM-GUID-4CB5B5E1-E853-4CA2-B43D-54CD18A8F28A>

Configurazione

Nelle tabelle che seguono sono riepilogati i valori di configurazione della risorsa cloud ExaDB-D Infrastructure, della quale è necessario effettuare il provisioning propedeutica al successivo provisioning degli ExaDB-D VM Clusters.

Configurazioni Mandatorie

Attributo	Ambiente Comune	Note
Compartment	cmp-exinfra	
Display Name	exa-infra-ares-01	
Availability Domain	AD1	
Infrastructure Model	X9M-2	
Database Servers	2	
Storage Servers	3	

Configurazioni per la Maintenance

La configurazione della schedulazione della maintenance non è mandatoria, la tabella fornisce indicazioni relative ai valori di default, che in caso di necessità è possibile personalizzare.

Attributo	Ambiente Comune	Note
Method	Rolling	
Schedule	No Preference	
Custom Action Enabled	No	
Custom Action timeout		

Maintenance Months

Quarter 1	Quarter 2	Quarter 3	Quarter 4
February	May	August	November
March	June	September	December
April	July	October	January

Altre configurazioni per lo scheduling della Maintenance

Attributo	Non-Produzione	Note
Week of the Month	Any Week	
Day of the Week	Any Day	
Hour of the Day (UTC)	Any Hour	
Notification lead time	2 weeks in advance	
Maintenance Contact email addresses		

Tagging

Tag Namespace	Tag Key	Tag Value

Exadata Cloud Service VM Cluster

Per la descrizione dei passi dettagliati per il provisioning di un VM Cluster Exadata, fare riferimento alla documentazione ufficiale, consultabile alla URL: <https://docs.oracle.com/en-us/iaas/exadatacloud/doc/manage-vm-clusters.html#ECSCM-GUID-11C092BB-2B85-4342-B143-8FC5FC80ECA3>

Networking

Nei paragrafi che seguono vengono riportate le configurazioni delle componenti di networking che forniscono la connettività necessaria al corretto funzionamento delle Virtual Machines componenti i VM Clusters ExaDB-D, ospitati dalle ExaDB-D Infrastructure descritte negli specifici paragrafi di questo documento.

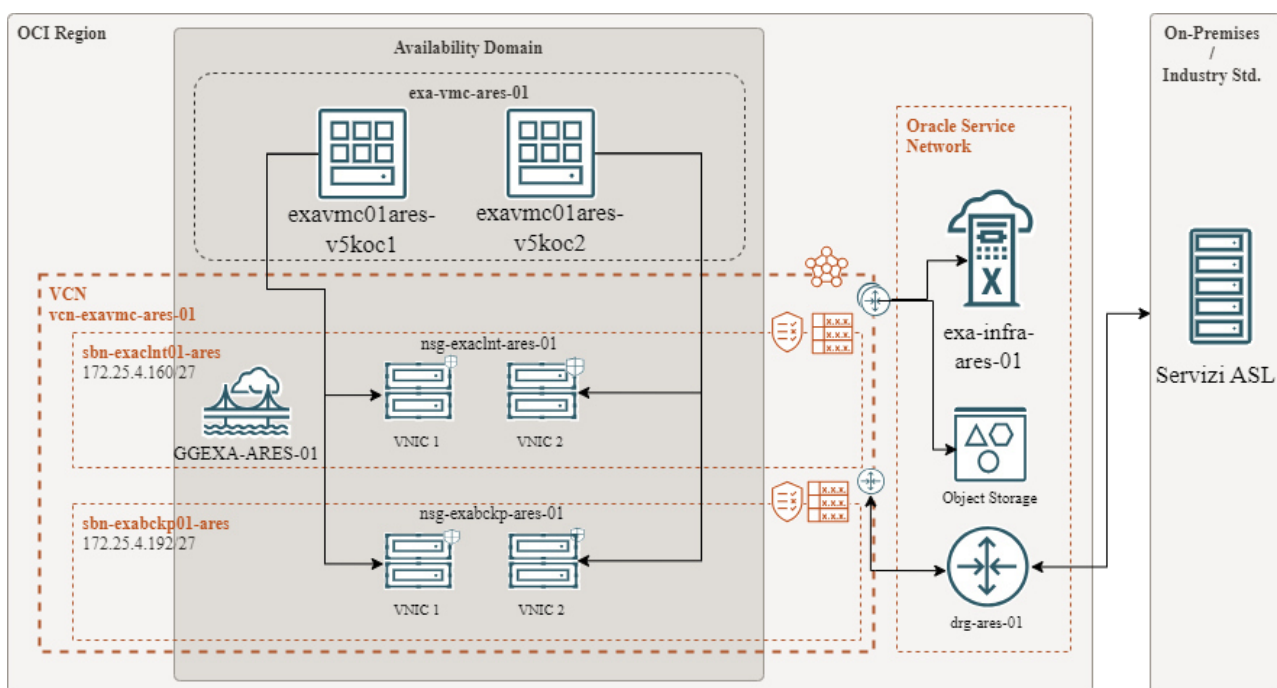


Figura 1 - Networking Architecture

Custom DNS Resolution

Per permettere il provisioning delle VM per i VM Clusters e dei successivi DNS names degli SCAN e servizi di rete degli Oracle Databases gestiti, con i corretti FQDN, relativi al dominio di appartenenza, è necessario configurare inizialmente il DNS Resolver della VCN configurata per ospitare il VM Cluster, in modo che possa aggiungere la corrispondenza VM-IP Address, con il FQDN appartenente al dominio di destinazione (aggiunta dinamica degli A Records), ciò è realizzato mediante la definizione in OCI di una private zone corrispondente al DNS name da assegnare, e una private view che punti alla private zone appena definita.

La private view verrà poi associata al DNS Resolver della VCN che ospiterà le subnets (client e backup) relative al VM Cluster ExaDB-D.

Le tabelle che seguono dettagliano i valori di configurazione di Private Views e Private Zones, per gli ambienti di non produzione e produzione:

Private View

Attributo	Ambiente Comune	Note
Name	pview-vcn-exa-ares-01	
Compartment	cmp-network	

Private Zone

Attributo	Ambiente Comune	Note
Zone Type	Primary	
Zone Name	Sisar.asl	
Compartment	cmp-network	
DNS private view	pview-vcn-exa-noprod-01	

Virtual Cloud Network

Definite le modalità di risoluzione dei DNS names, è possibile creare gli oggetti di rete, necessari al provisioning dei VM Cluster ExaDB-D.

Le tabelle che seguono elencano e descrivono le VCNs, suddividendole per ambienti: Non Produzione e Produzione.

Attributo	Ambiente Comune	Note
Compartment	cmp-network	
Display Name	vcn-exavmc-ares-01	
CIDRs	172.25.4.160/27 + 172.25.4.192/27	
Indirizzi IP utili	64	
Associated private views	pview-vcn-exa-ares-01	

Di seguito i valori di configurazione delle Subnets da predisporre, relative alle VCNs descritte nei paragrafi precedenti:

Client Subnets

Attributo	Ambiente Comune	Note
VCN	vcn-exavmc-ares-01	
Compartment	cmp-network	
Name	sbn-exaclnt-ares-01	
Subnet Type	Regional	
IPv4 CIDR Block	172.25.4.160/27	
Hosts	30	
Subnet Access	Private	

Backup Subnets

Attributo	Ambiente Comune	Note
VCN	vcn-exavmc-ares-01	
Compartment	cmp-network	
Name	sbn-exabckp-ares-01	

Subnet Type	Regional	
IPv4 CIDR Block	172.25.4.192/27	
Hosts	30	
Subnet Access	Private	

Gateways

Per permettere la configurazione dei servizi all'interno del contesto di rete definito dalle VCNs e relative Subnets, è necessario effettuare il provisioning di gateways di rete che permettano la comunicazione con i servizi necessari nella Oracle Services Network al loro corretto provisioning e funzionamento.

Service Gateway

Attributo	Ambiente Comune	Note
VCN	vcn-exavmc-ares-01	
Compartment	cmp-network	
Name	sgw-exa-ares-01	

Security Lists e Routing Tables

Per consentire il raggiungimento della Oracle Services Network, attraverso il Service Gateway definito, è necessario configurare opportunamente security lists e rotte di rete per la VCN di riferimento dei VM Cluster.

Security List

Attributo	Ambiente Comune	Note
Security List Name	Default Security List for vcn-exavmc-ares-01	
Compartment	cmp-network	

Ingress Rules

Attributo	Ambiente Comune	Note
Source Type	Service	
Source Service	All <region> Services in Oracle Services Network	
IP Protocol	TCP	
Source Port Range	All	
Destination Port Range	All	
Source Type	CIDR Block	
Source Address Range	10.0.0.0/8; 172.25.4.160/27	
IP Protocol	TCP	
Source Port Range	All	
Destination Port Range	22, 1521	Accesso a VM via SSH / SQL*Net
Source Type	CIDR Block	
Source Address Range	10.0.0.0/8; 172.25.4.160/27	
IP Protocol	TCP	
Source Port Range	443	Accesso a Goldengate da rete ASL e PSN

Egress Rules

Attributo	Ambiente Comune	Note
Source Type	Service	
Destination Service	All <region> Services in Oracle Services Network	
IP Protocol	TCP	
Source Port Range	All	
Destination Port Range	All	

Routing Table

Attributo	Ambiente Comune	Note
Routing Table Name	Default Routing Table for vcn-exavmc-ares-01	
Compartment	cmp-network	

Route Rules

Attributo	Ambiente Comune	Note
Target Type	Service	
Destination Service	All <region> Services in Oracle Services Network	
Target Service	sgw-exa-ares-01	
Target Type	Local Peering Gateway	
Destination Address Range	100.65.0.240/28	
Destination LPG	lpg-exa-ares-01	LPG per raggiungibilità sistemi PSN (backup, ekm, ...)
Target Type	Dynamic Routing Gateway	
Destination Address Range	0.0.0.0/0	Rotte indicate via BGP dalla Fastconnect vs Industry Std.
Target	drg-ares-01	

Configurazione Exadata Cluster

Le tabelle che seguono elencano i valori di configurazione per la risorsa ExaDB-D VM Cluster, relativa alla Infrastructure definite nei paragrafi precedenti.

Attributo	Ambiente Comune	Note
Compartment	cmp-database	
Name	exa-vmc-ares-01	
Exadata Infrastructure	exa-infra-ares-01	
Oracle Grid Infrastructure Version	19c	
Numero di OCPU allocate per VM		
Memoria RAM allocata per VM	1250 GB	
Storage Locale per VM	400 GB	
Storage Exadata Usabile	80 TB	
Allocazione Storage per Sparse Snapshot	Non selezionato	
Allocazione Storage per Backup Locale	Non selezionato	
VCN	vcn-exavmc-ares-01	

Client Subnet	sbn-exacInt-ares-01	
Backup Subnet	sbn-exabckp-ares-01	
Utilizzo DNS privato	Selezionato	
Private View	pview-vcn-exa-ares-01	
Private Zone	Sisar.asl	
Prefisso Hostname	vmcares01	
Tipo di Licenza	Bring Your Own License (BYOL)	
Eventi Diagnostici	Abilitato	
Monitoraggio della Salute	Abilitato	
Log Incidents e Tracciamento	Abilitato	
Time zone	UTC	
Porta SCAN Listener	1521	
Hostname Nodo 1	exavmc01ares-v5koc1.sisar.asl	
Private IP Nodo 1	172.25.4.172	
Hostname Nodo 2	exavmc01ares-v5koc2.sisar.asl	
Private IP Nodo 2	172.25.4.185	
Floating IP	172.25.4.190 172.25.4.180	Default Nodo 1 Default Nodo 2

Configurazione Oracle Goldengate

La tabella seguente rappresenta la configurazione del servizio Goldengate in uso per la migrazione

Attributo	Ambiente Comune	Note
Compartment	cmp-database	
Name	GGEXA-ARES-01	
Username	ADMINARES	
Password secret	GGPWDSECRETARES	
Secret location	cmp-security	
Console URL	https://i2ujk7ey7rqa.deployment.goldengate.eu-dcc-rome-1.oci.psn-pco.it/	
IP Locale	172.25.4.165	
IP Ingress	172.25.4.182, 172.25.4.176	
Subnet	Sbn-exacInt01-ares	
OCPU	8	
Auto Scaling	Disables	
License Type	License Included	
OGG Version	Oggoracle:21.17.0.0.0_250125.0558_1192	

Configurazione Oracle Database

Attributo	Ambiente Comune	Note
SCAN DNS Name	exavmc01ares-v5koc-scan.sisar.asl	
SCAN IP	172.25.4.164 172.25.4.170 172.25.4.166	
DB Home Version	19.22.0.0	Comune a tutti i DB
DB Home	dbhome_asl1_ares dbhome_asl2_ares dbhome_asl3_ares dbhome_asl4_ares	

	dbhome_asl5_ares dbhome_asl6_ares dbhome_asl7_ares dbhome_asl8_ares dbhome_aouca_ares dbhome_aouss_ares dbhome_crestest_ares dbhome_arnas_ares	
CDB	ASL1CDB ASL2CDB ASL3CDB ASL4CDB ASL5CDB ASL6CDB ASL7CDB ASL8CDB AOUCACDB AOUSSCDB CRESTCDB BROTZUCDB	
PDB	ASL1PDB ASL2PDB ASL3PDB ASL4PDB ASL5PDB ASL6PDB ASL7PDB ASL8PDB AOUCAPDB AOUSSPDB CRESTPDB BROTZUCDB	
Metodologia Chiave di cifratura	Customer-Managed key	
Chiave di Cifratura	key-1-fqdn	
Compartment Chiave di cifratura	cmp-servicecompartment/cmp-security	