



SMMePlus

System Infrastructure

V4.0

This document contains proprietary information of Enel Global Digital Solutions and should only be used by the recipient in relation to the purposes for which it was received. Any form of reproduction or dissemination is forbidden without the express consent of Enel Global Digital Solutions.

Redatto da:	Federica Di Rienzo	12/05/2020
Verificato da:		12/05/2020
Approvato da:		-

Summary

The aim of this document is to describe the infrastructure of SMMePlus environments

References

List of the documents

- [1] SMMePlus - Architecture → SMMePlus - Architecture v4.0.pdf

Index

1.	Introduction	4
1.1.	Purpose	4
2.	Infrastructure	5
2.1.	Service Fabric.....	5
2.1.1.	Operator System	5
2.2.	Database	6
2.2.1.	Type	6
2.2.2.	Azure SQL Autiding.....	6
2.2.3.	Backup and restore	7
2.2.4.	Data Encription.....	8
2.3.	Website	9
2.4.	Collected information.....	9
3.	Log	10
3.1.	Website	10
3.2.	Backend	10
3.3.	Database	10
3.4.	Report	11
4.	Configuration	12
4.1.	PRO 1 Configuration.....	12
4.1.1.	Service Fabric Cluster	12
4.1.2.	External Load Balancer	12
4.1.3.	Internal Load Balancer	12
4.1.4.	Website	12
4.1.4.1.	URL	12
4.1.4.2.	Application service environment.....	12
4.1.5.	Wake up listener.....	12
4.1.5.1.	Chile.....	12
4.1.6.	Database.....	12

1. Introduction

1.1. Purpose

The aim of this document is to describe the infrastructure of SMMePlus system.

2. Infrastructure

2.1. Service Fabric

SMMePlus system is a Service Fabric Application backed by several virtual servers that form a Service Fabric Cluster. This set of virtual machines hosts microservices and Service Fabric Runtime.

Availability and efficiency are granted by replication of service's state and distribution of replicas among different machines.

More information about Service Fabric are available at <https://docs.microsoft.com/en-us/azure/service-fabric/>.

2.1.1. Operator System

The operator system of the servers of the cluster is Windows Server 2016 Datacenter

2.2. Database

2.2.1. Type

The database of SMMePlus are SQL Azure (DB as a Service)

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-technical-overview>

The database doesn't store all the commercial information.

Only few commercial information (last reading and last credit for each meter) are kept in database for being shown in report.

2.2.2. Azure SQL Auditing

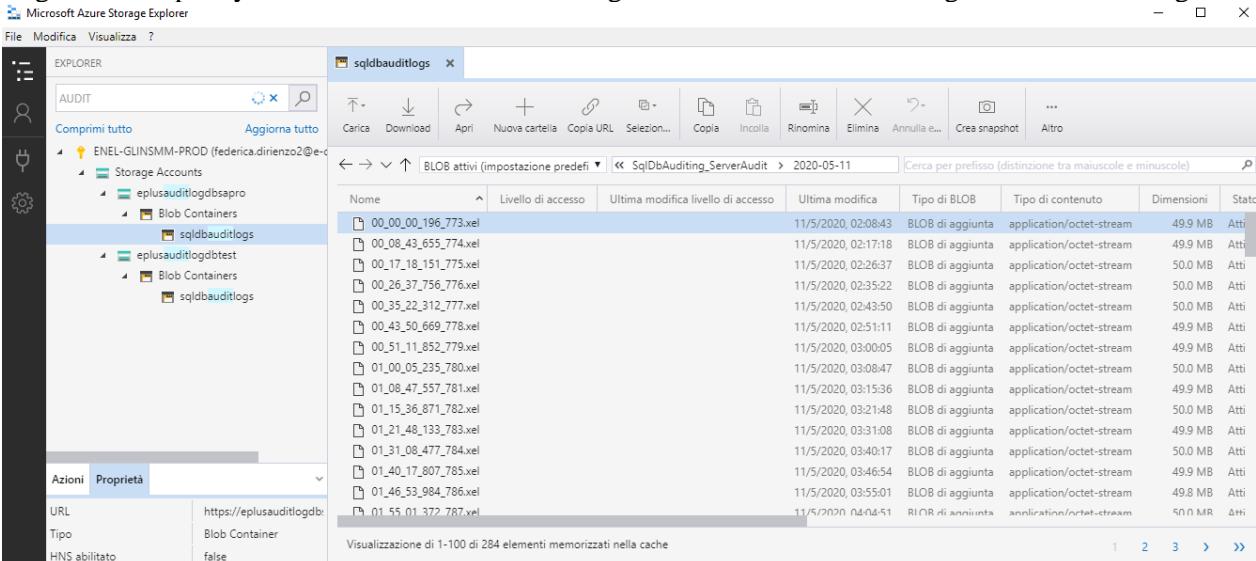
On production server (smmeplus-db-sa-server.database.windows.net) the Auditing feature is enabled with default policy.

The default auditing policy includes all actions and the following set of action groups, which will audit all the queries and stored procedures executed against the database, as well as successful and failed logins:

- BATCH_COMPLETED_GROUP
- SUCCESSFUL_DATABASE_AUTHENTICATION_GROUP
- FAILED_DATABASE_AUTHENTICATION_GROUP

<https://docs.microsoft.com/en-us/azure/sql-database/sql-database-auditing>

Logs of Audit policy are stored on Azure File Storage, that can be accessed using a connection string.



The screenshot shows the Microsoft Azure Storage Explorer interface. On the left, the 'EXPLORER' pane displays a tree view of storage accounts. Under the 'Storage Accounts' section, 'eplusauditlogdbtest' is expanded, showing 'Blob Containers' and 'sqlauditlogs'. The 'sqlauditlogs' container is selected. On the right, the 'sqlauditlogs' pane shows a list of audit log files. The table has columns: Nome (Name), Livello di accesso (Access level), Ultima modifica (Last modified), Tipo di BLOB (blob type), Tipo di contenuto (Content type), Dimensioni (Size), and Stato (Status). The list includes numerous files named like '00_00_00_196_773.xel', '00_08_43_655_774.xel', etc., with sizes ranging from 49.9 MB to 50.0 MB and all marked as 'Atti' (Active).

Nome	Livello di accesso	Ultima modifica	Tipo di BLOB	Tipo di contenuto	Dimensioni	Stato
00_00_00_196_773.xel		11/5/2020, 02:08:43	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
00_08_43_655_774.xel		11/5/2020, 02:17:18	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
00_17_18_151_775.xel		11/5/2020, 02:26:37	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
00_26_37_756_776.xel		11/5/2020, 02:35:22	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
00_35_22_312_777.xel		11/5/2020, 02:43:50	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
00_43_50_669_778.xel		11/5/2020, 02:51:11	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
00_51_11_852_779.xel		11/5/2020, 03:00:05	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
01_00_05_235_780.xel		11/5/2020, 03:08:47	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
01_08_47_557_781.xel		11/5/2020, 03:15:36	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
01_15_36_871_782.xel		11/5/2020, 03:21:48	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
01_21_48_133_783.xel		11/5/2020, 03:31:08	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
01_31_08_477_784.xel		11/5/2020, 03:40:17	BLOB di aggiunta	application/octet-stream	50.0 MB	Atti
01_40_17_807_785.xel		11/5/2020, 03:46:54	BLOB di aggiunta	application/octet-stream	49.9 MB	Atti
01_46_53_984_786.xel		11/5/2020, 03:55:01	BLOB di aggiunta	application/octet-stream	49.8 MB	Atti
01_55_01_372_787.xel		11/5/2020, 04:44:51	RITORNI DI AGGIUNTA	application/octet-stream	50.0 MB	Atti

The files can be downloaded and opened with SQL Server Management Studio.

It's possible to explore the Audit policy logs also in Azure portal.

The screenshot shows the Azure Log Analytics interface for the SMMePlus_SAPRO_DB database. On the left, there is a table titled "Audit records" showing a list of audit events. The columns include Event time (UTC), Principal name, Event type, and Action status. Most events show SMM_APP_USER as the principal, RPC COMPLETED as the event type, and Succeeded as the action status. The first event is dated 5/12/2020 1:30:16 PM. On the right, there is a detailed view of a single audit record for the same timestamp. It shows the event time as 5/12/2020 1:30:16 PM, event type as RPC COMPLETED, and server name as smmplus-db-sa-server. The application name is .Net SqlClient Data Provider, and the principal name is SMM_APP_USER. The client IP is 23.101.66.200, and the status is Succeeded. Below this, a "STATEMENT" section shows the SQL command: `exec [TECH].[usp_GetMeterDataByIdMeterField] @idmeterfield=651091`.

Only users configured for accessing the Azure Portal and enabled on subscription

The screenshot shows the Azure IAM Access control (IAM) blade for the ENEL-GLINSMM-PROD subscription. The left sidebar lists various management categories like Overview, Activity log, and Access control (IAM). The main area displays a table of contributors. The columns include a profile picture, name, role, and resource. The contributors listed are Alessandro Bigi (Guest), aleppan (Guest), Andrea Uggenti (Guest), Adatti Sonia (EXT Infodue), Campofranco Arturo (I&N DH), Di Rienzo Federico (I&N DH), Calvi Marco (I&N DH), GG-SH-AZURE-Enel-AllSub-Datacenter, Merlini Guido (I&N DH), Marta Fausti (Guest), and Nazareno Lamparelli (Guest). All contributors are assigned the Contributor role and have access to This resource.

2.2.3. Backup and restore

SQL Database uses SQL Server technology to create full backups every week, differential backups every 12 hours, and transaction log backups every 5-10 minutes. The backups are stored in RA-GRS storage blobs that are replicated to a paired data center for protection against a data center outage. When you restore a database, the service figures out which full, differential, and transaction log backups need to be restored.

The Point in Time recovery is available for 35 days.

The Long Time recovery is configured as following:

- Weekly backup available for 6 months
- Monthly backup available for 1 year

2.2.4. Data Encryption

Transparent data encryption is enabled.
This feature encrypts databases, backups, and logs.
Here are more details:
<https://docs.microsoft.com/it-it/azure/sql-database/transparent-data-encryption-azure-sql?view=sql-server-ver15&tabs=azure-portal>

2.3. Website

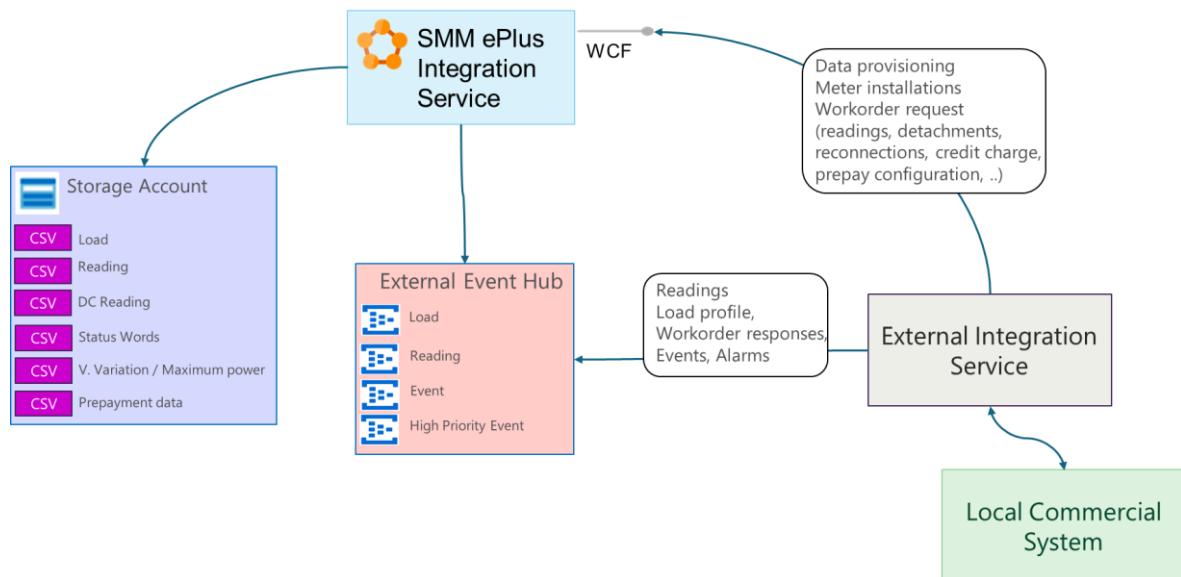
In UAT and Production environment, the websites are hosted in Azure Application Service Environment. The Environment is mapped in Enel domain **enelint.global** and website can be reached only from Enel network.

<https://docs.microsoft.com/it-it/azure/app-service/environment/intro#overview>

2.4. Collected information

As described in SMMePlus – Architecture (Reference [1]), the information collected by SMMePlus are available for local business in two ways:

- csv files for each day for readings, daily closures, load profiles, prepayment information, maximum powers
- pushes data on external Event Hubs so that external services can download them asynchronously



CSV are available on Storage Account. Each storage account contains information of a single company and can be accessed with a connection string.

The Event Hub is a cloud stream on which it is possible to subscribe using a specific consumer identification and key.

3. Log

3.1. Website

Each website logs activities in a text file per each day.

This is an example of log file. It refers to 7th of May in UAT environment.



SMMePlus.WP-2020
0507.log

This is an example of log file. It refers to 8th of May in PRO2 environment.



SMMePlus.WP-2020
0508.log

This is an example of log file. It refers to 5th of May in PRO environment.



SMMePlus.WP-2020
0505.log

These files are saved in the same FTP folder of the web site and are never deleted.

To access the FTP it's required the username and the password.

3.2. Backend

The services in backend logs in text files in the file system of the servers.

These logs are used in case of specific analysis, usually if an activity has some problems in execution.

To access these logs it's necessary to have local access to servers of the cluster.

3.3. Database

As described in section 2.2.2 SQL Auditing, the SQL Auditing feature is enabled and writes on Azure Storage Explorer the logs of queries and stored procedure, success and failed log in.

3.4. Report

In SMMePlus website, reports are used to check results of activities in the system.

Here are some information extracted from database.

In following files, it's possible to see activities executed on 29th of April.

extraction_workordercompleted_2020-04-29.csv

extraction_workcompleted_2020-04-29.csv



extraction_workco extraction_workord extraction_profileus
mpleted_2020-04-29ercompleted_2020-0 er.csv

Workorders are remote activities on meters.

Works are remote activities on concentrators. A work can have several workorders associated, in case the concentrator has to forward to meters the activityes.

In extraction_provisioningfile_2020-04-21.csv it's possible to see an example of csv file uploaded by the user in the system.



extraction_provisio
ningfile_2020-04-21.

This information are stored in database.

For accessing database it's necessary to:

- Have the username and password
- Have the source ip address enabled in firewall

4. Configuration

4.1. PRO 1 Configuration

4.1.1. Service Fabric Cluster

Cluster name: smmeplus-sfclu-sa-pro

Node 0	10.132.20.196	23.101.66.200:3389
Node 1	10.132.20.197	23.101.66.200:3390
Node 2	10.132.20.198	23.101.66.200:3391
Node 3	10.132.20.199	23.101.66.200:3392
Node 4	10.132.20.200	23.101.66.200:3393

4.1.2. External Load Balancer

23.101.66.200 (LBIP-smmeplus-sfclu-sa-pro-0)

4.1.3. Internal Load Balancer

10.132.20.228

4.1.4. Website

4.1.4.1. URL

<https://smmeplus-web-sapro.enelint.global/>

4.1.4.2. Application service environment

Domain enelint.global (10.132.20.75)

4.1.5. Wake up listener

4.1.5.1. Chile

10.132.20.228

Port: 58692

4.1.6. Database

Server: smmeplus-db-sa-server.database.windows.net

Read-only server: smmeplus-db-sa-ro-server.database.windows.net