GridOps Management Suite 3.10

Seamless Site Switch Interface

Functional Specification

Document Version: 1.1

Updated: June, 2024

Table of Contents

Table of Figures

Table of Tables

Table of Documents

No table of figures entries found.

1. REFERENCES

#	Title	Description
1.	EcoStruxure GridOps Management Suite 3.10 Enterprise Integration Platform - Functional Specification	The document represents a set of common integration principles applied to all baseline integration adapters.
2.	EcoStruxure GridOps Management Suite 3.10 Seamless Site Switch Interface	EcoStruxure GridOps Management Suite 3.10 Seamless Site Switch Interface zip file contains essential configuration information, as well as message examples.

2. INTRODUCTION

EcoStruxure GridOps Management Suite is a family of solutions designed to help electric utilities in the operations and management of their grid. It is offered as EcoStruxure ADMS, EcoStruxure Grid Operation, EcoStruxure DERMS or EcoStruxure Energy Transmission Operation solutions, which share the same technology platform.

NOTE: The functionality described in this document applies to all solutions.

NOTE: Most images presented in this document are related to the EcoStruxure ADMS solution and should be used as an example. The images for other solutions may differ slightly.

Seamless Site Switch Interface provides information about currently active site instance. It is subscribed to site mode changes and stores the information of currently active site. Most common use case for this interface is integrating with a network load balancing application used for balancing DNS traffic for integration interfaces. SSS Interface implements a logic to be used by load balancer to check which site is active and properly route DNS traffic to the currently active site. With this interface, the site switch process of integration components is automated.

2.1. General Architecture

Described in the *EcoStruxure GridOps Management Suite 3.10 Enterprise Integration Platform - Functional Specification* [1].

The specific architecture of SiteSwitch integration solution is given in Figure 2.1.

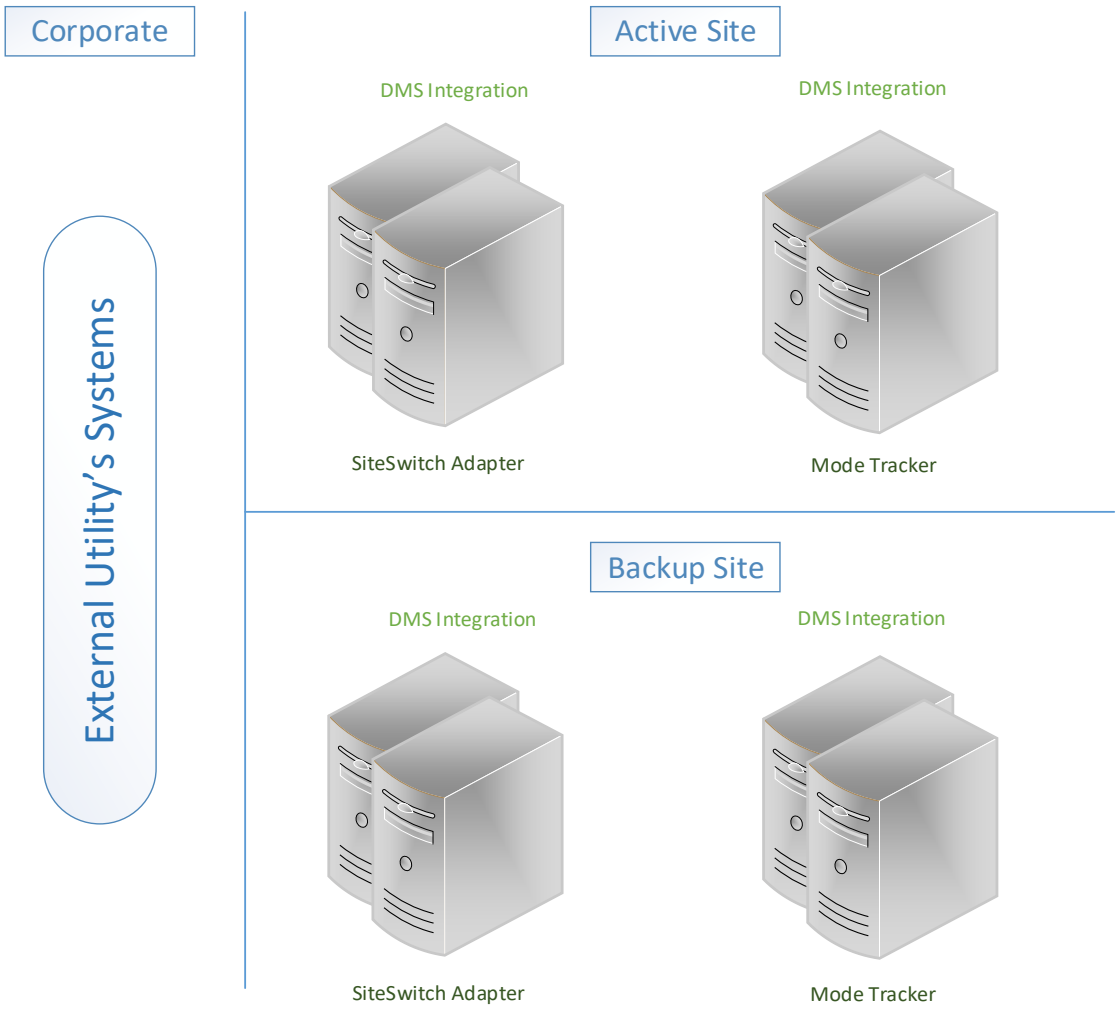

Figure 2.1 – The General Architecture of SiteSwitch integration

3. OVERVIEW

SSS Integration is implemented through the SiteSwitch Adapter component. The aforementioned adapter implements a RESTful web service for providing information about currently active site. Service implements a single operation:

- IsActive service operation – Used for querying information about the currently active site. The data about currently active instance is received from Mode Tracker component via event publication. Adapter is subscribed to the Mode Switch change and updates the state internally upon receiving publication.

SiteSwitch adapter is available on HOT server on both sites. Invoking the service on the adapter on active sites returns a positive response, signaling that site is currently active. Invoking the service on the adapter on backup site returns a negative response. Both positive and negative responses are represented with corresponding HTTP status codes.

The following chapters provide more details regarding briefly described interface above, along with the service operation, error handling scenarios, etc.

The use case diagram that represents common participants (actors) and users of the aforementioned interface in the SSS Integration is given in Figure 3.1.

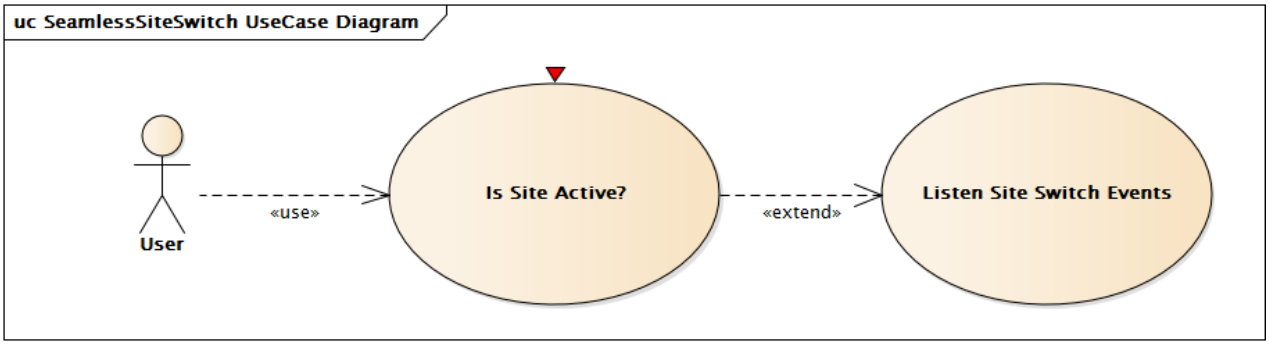

Figure 3.1 –SSS Integration use case diagram

4. FUNCTIONALITY

4.1. SiteSwitch Service

4.1.1. IsActive Service Operation

4.1.1.1. Overview

As stated above SiteSwitch is a RESTful web service designed for retrieving information about currently active site. Service is hosted on the EcoStruxure GridOps side. It implements a request-response integration pattern. The information is fed to the adapter from a dedicated service that handles site switch operation. Adapter is subscribed to these events. Upon receiving publication, SSS adapter stores the information internally. IsActive service operations returns this value upon invocation. Visual representation of the process is visible on Figure 4.1.

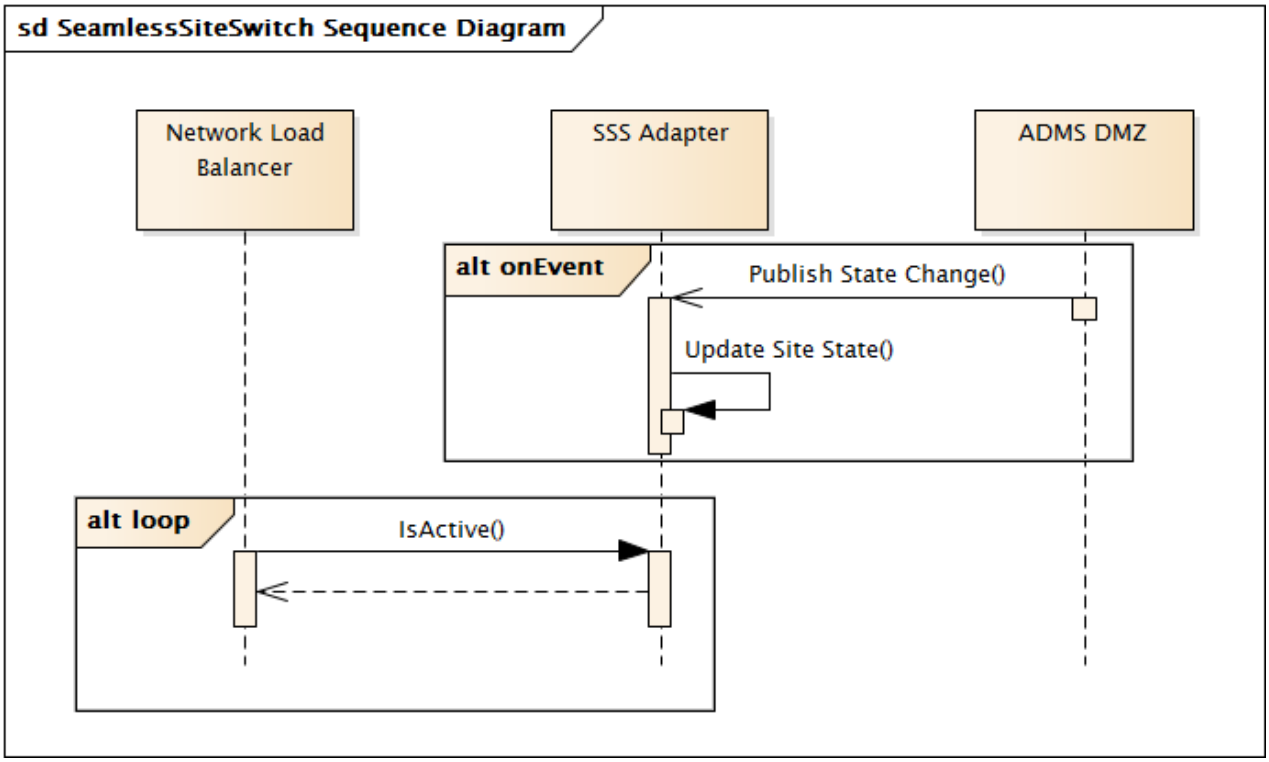

Figure 4.1 –SSS Integration Sequence Diagram

SiteSwitch service operation supports service auditing. Service auditing represents a process dedicated for monitoring the usage rate of the service. If the service operation has not been invoked for a configurable period of time, an event (or alarm) is created which will indicate the existence of a potential communication error between the adapter and the external service client. Service Auditing is configurable within adapter registry configuration file.

4.1.1.2. Use Cases

Table 4.1 – The list of possible use cases and corresponding faults

Use Case	Message Mapping			Action
	Property	Type	Value	
Querying site state succeeded. Site is Active.	Result	String	OK	External system sends request message to the adapter running on the active site. Response is returned with the HTTP Status Code 200 (OK)
	Error.code	String	N/A	
	Error.level	String	N/A	
	Error.reason	String	N/A	
	Error.details	String	N/A	
Querying site state succeeded. Site is Inactive.	Result	String	OK	External system sends request message to the adapter running on the backup (non-active) site. Response is returned with the HTTP Status Code 503 (Service Unavailable)
	Error.code	String	N/A	
	Error.level	String	N/A	
	Error.reason	String	N/A	
	Error.details	String	N/A	
Service was not invoked for a configurable period of time.	Result	String	N/A	External system does not send request messages for a time period that exceeds predefined auditing criteria. An event (or Alarm, depends on configuration parameter) is created and visible in the corresponding summary in CORE system.
	Error.code	String	N/A	
	Error.level	String	N/A	
	Error.reason	String	N/A	
	Error.details	String	N/A	
Querying site state failed. SiteSwitch service is unavailable.	Result	String	FAILED	External system sends request message to the adapter that should be running on active site, but it is unavailable. Response is returned to the invoker with HTTP Status Code 404.
	Error.code	String	N/A	
	Error.level	String	N/A	
	Error.reason	String	N/A	
	Error.details	String	N/A	

5. DEPLOYMENT SPECIFICATION

SiteSwitch Adapter provides integration between the EcoStruxure GridOps and clients external applications such as: Web Service Clients, NLB's, etc. Process is invoked on the various services via intranet WCF service invocation.

The deployment specification is provided in the following table:

Table 5.1 – The deployment specification

Deployment Specification	
Application	EmailAdapter
Critical process	No
OASyS service	OASyS DNA DMS_INTEGRATION Service
Servers	pdmz-int-1, pdmz-int-2, bdmz-int-1, bdmz-int-2
Zone	pdmz, bdmz
Installation Type	Product
Installation add-on name	Integration Adapters

Figure 5.1 depicts standard deployment configuration for all SSS Integration participants.

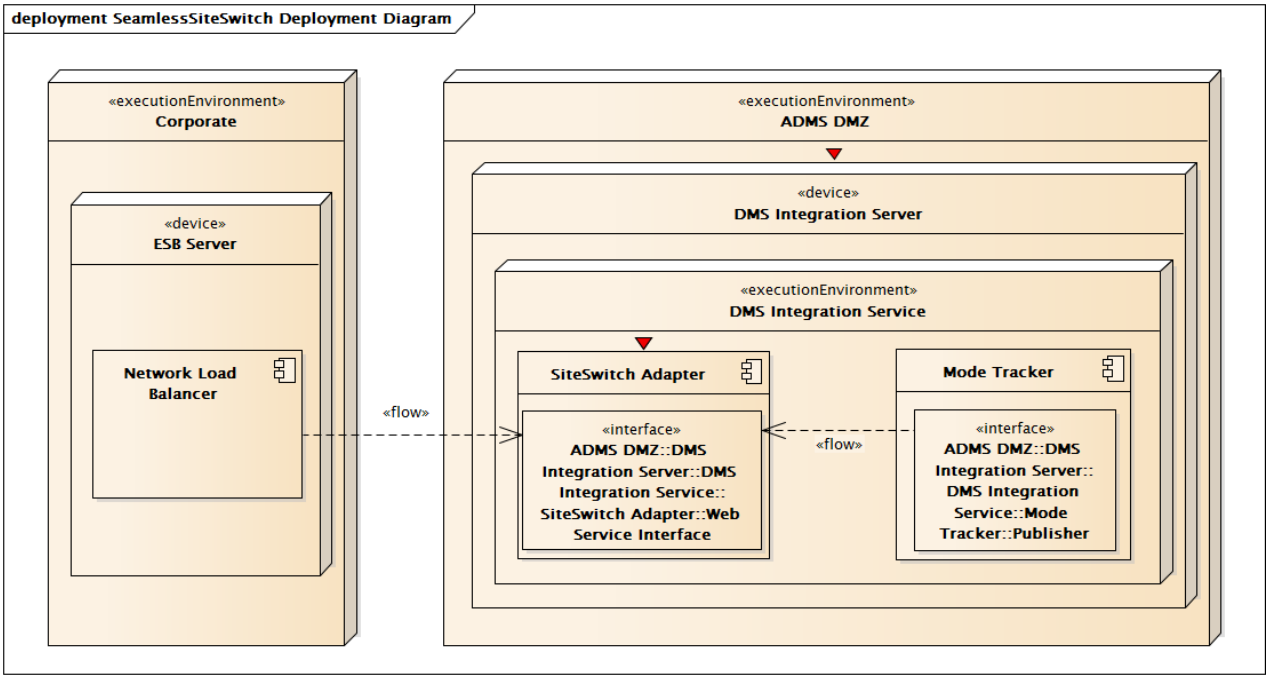

Figure 5.1 –SiteSwitch Adapter deployment diagram

5.1. Interface Configuration

For the establishment of the end-to-end connection, the appropriate information needs to be provided from both sides. The virtual host names and virtual IP addresses of the DMS_Integration service on different sites are given in the following table.

Table 5.2 – The DMS_Integration service information

Site	Virtual Host Name	Virtual IP Address
Primary	pdmzDMS_Integration	TBD
Backup	bdmzDMS_Integration	TBD

The Virtual IP Address is related to one pair of servers (Hot/Stand by). In case of a failover, the Stand By server becomes Hot but the IP address used for accessing the web service stays the same. Therefore, the client applications are not aware of the failover. This is provided by the OASyS infrastructure and the Arbitration service. More details about the system configuration can be found in the appropriate System Configuration Plan document.

In order for external systems to access the SiteSwitch Adapter web services, the appropriate information needs to be provided. The information about their addresses hosted within the SiteSwitch Adapter which runs under the DMS_Integration service on one of the DMS Integration servers is provided in the following table.

Table 5.3 – The web service information

Web Service Name	URL
SiteSwitchService	http(s)://{DMSIntegrationServiceIPAddress} : {Port} / SiteSwitchService / DMSIntegration / HealtCheckActive

Usually, ports on which aforementioned web services are hosted are proposed by the client. If the client does not have any requirements (preferences) regarding the port number, it will be chosen by Schneider Electric DMS.

SSS adapter provides certain amount of configurability so that smaller adjustments in the functionality can be easily applied to the system, without interface down time. Such feature is provided through dedicated configuration files of the SSS adapter.

Details about the structure and shared content of common interface configuration files are located in *EcoStruxure GridOps Management Suite 3.10 Enterprise Integration Platform - Functional Specification* [1]

Detailed content of above-mentioned configuration files is provided within the *Configuration* folder in the *EcoStruxure GridOps Management Suite 3.10 Seamless Site Switch Interface.zip* file [2].

6. APPENDIX

6.1. Message Examples

Message examples for several use cases are provided within the *Message Examples* folder in the *EcoStruxure GridOps Management Suite 3.10 Seamless Site Switch Interface.zip* file [2].

6.2. F5 Load Balancer Configuration

This section describes how to setup the BIG IP F5 load balancer.

6.2.1. Nodes

A node is a logical object on the BIG-IP Local Traffic Manager system that identifies the IP address of a physical resource (web server) on the network.

Nodes should be created for virtual IP addresses on active and backup site. Here are steps for creating nodes as well as visual presentation on Figure 6.1:

1. On the Main tab, click **Local Traffic → Nodes → Node List**.
2. Click **Create**.
3. In the **Name** field, type a name for the node.
4. In the **Address** field, type an (virtual) IP address of node.
5. Click **Finished**.
6. Repeat for (virtual) IP address of backup site.

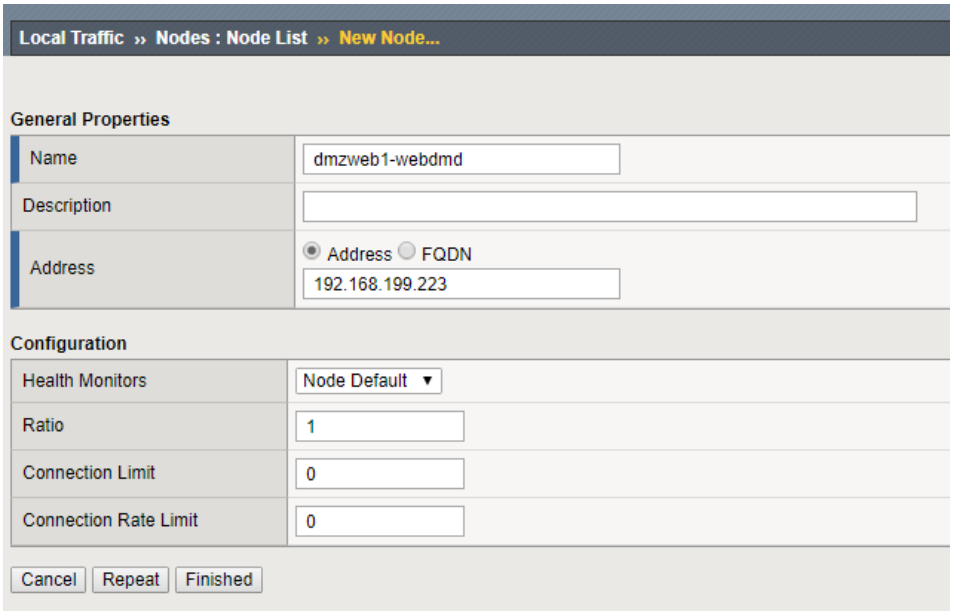

Figure 6.1 – F5 LB Configuration: Creation of new node

6.2.2. Monitors

The BIG-IP system uses monitors to check whether or not pool members are eligible to service application traffic. Monitors periodically send specific requests to pool members and evaluate their health based on the members' response or lack thereof.

Here are steps to create Monitor. Visual representation is presented on Figure 6.2:

1. On the Main tab, click **Local Traffic** → **Monitors**.
2. Click **Create**.
3. In the **Name** field, type a name for monitor (e.g. *TestSystemName*_Site_isActive).
4. In the **Type** field, select HTTP.
5. In the **Interval** field, set value agreed with client. Interval filed specifies, in seconds, the frequency at which the system issues the monitor check when either the resource is down or the status of the resource is unknown.
6. In the **Timeout** field, set value agreed with client. Specifies the number of seconds the target has in which to respond to the monitor request. If the target responds within the set time period, it is considered up. If the target does not respond within the set time period, it is considered down.
7. In the **Send String** field, type "GET *AdapterServiceEndpointPath* /\r\nHost: *Domain*".
8. In the **Receive String** field, type "200 OK".
9. In the **Alias Service Port** field, select HTTP.
10. Click **Finished.**

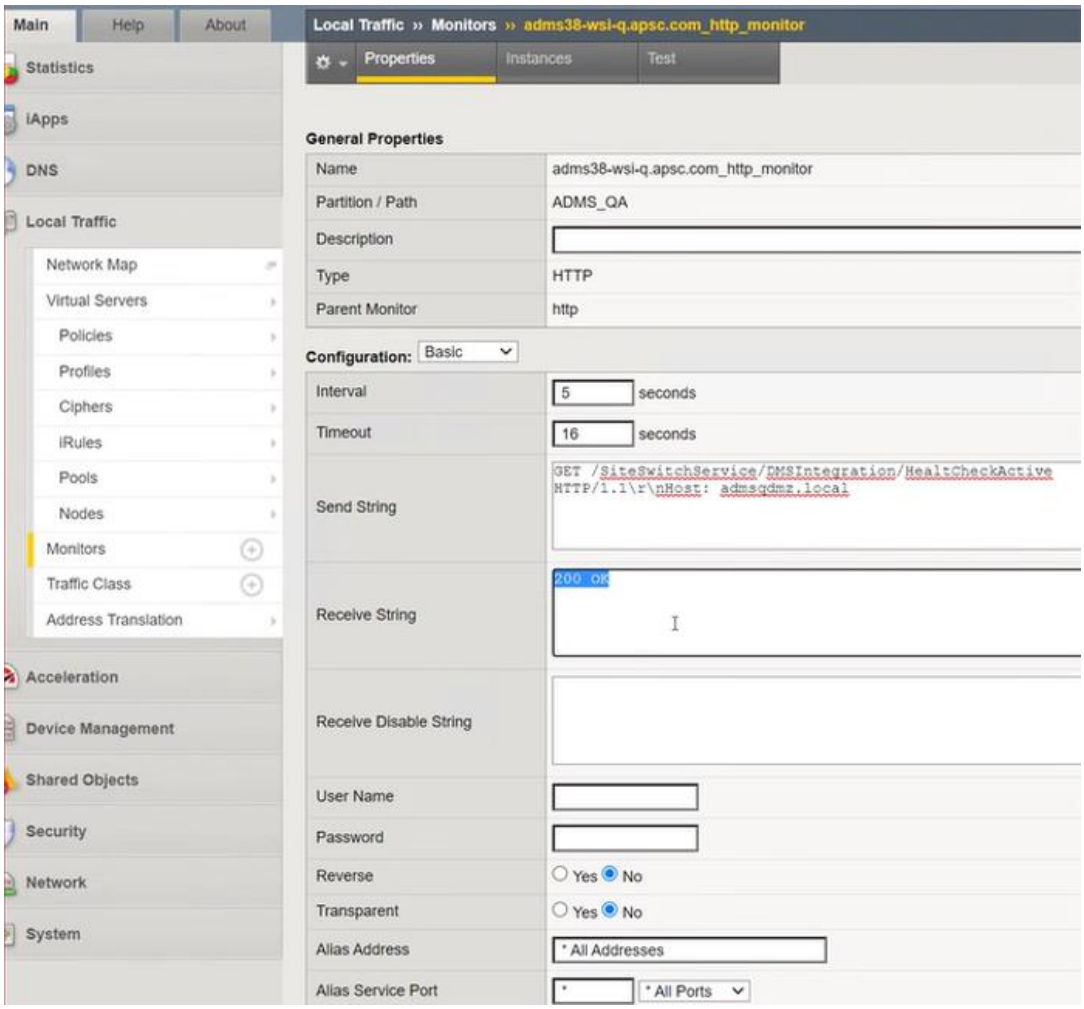

Figure 6.2 – F5 LB Configuration: Creation of new monitor

6.2.3. Pools

A pool is a logical set of devices, such as web servers, that you group together to receive and process traffic. A Pool consists of pool members. A pool member is a logical object that represents a physical node on the network. The difference between a node and a pool member is that a node is designated by the devices IP address only (10.10.10.10), while designation of a pool member includes an IP address and a service (such as 10.10.10:80).

The default method for load balancing on the BIG-IP system is Round Robin. It works best when the pool members are roughly equal in processing and memory capacity and application requests use server resources uniformly. Visual representation is provided in Figure 6.3.

1. On the Main tab, click **Local Traffic > Pools → Pools List**.
2. Click **Create**.
3. In the **Name** field, type a name for the pool.
4. In the **Health Monitors** field, select health monitor for pool (created in 6.2.2 Monitors).
5. In the **Load Balancing Method** field, select Round Robin.
6. In the **New Members** field, select Node List

a. Select **Address** created in 6.2.1 Nodes
b. For **Service Port** field, type port number on which adapter is hosting its service and select HTTP then click **Add**.
c. Repeat step 6 for all nodes.

7. Click **Finished.**

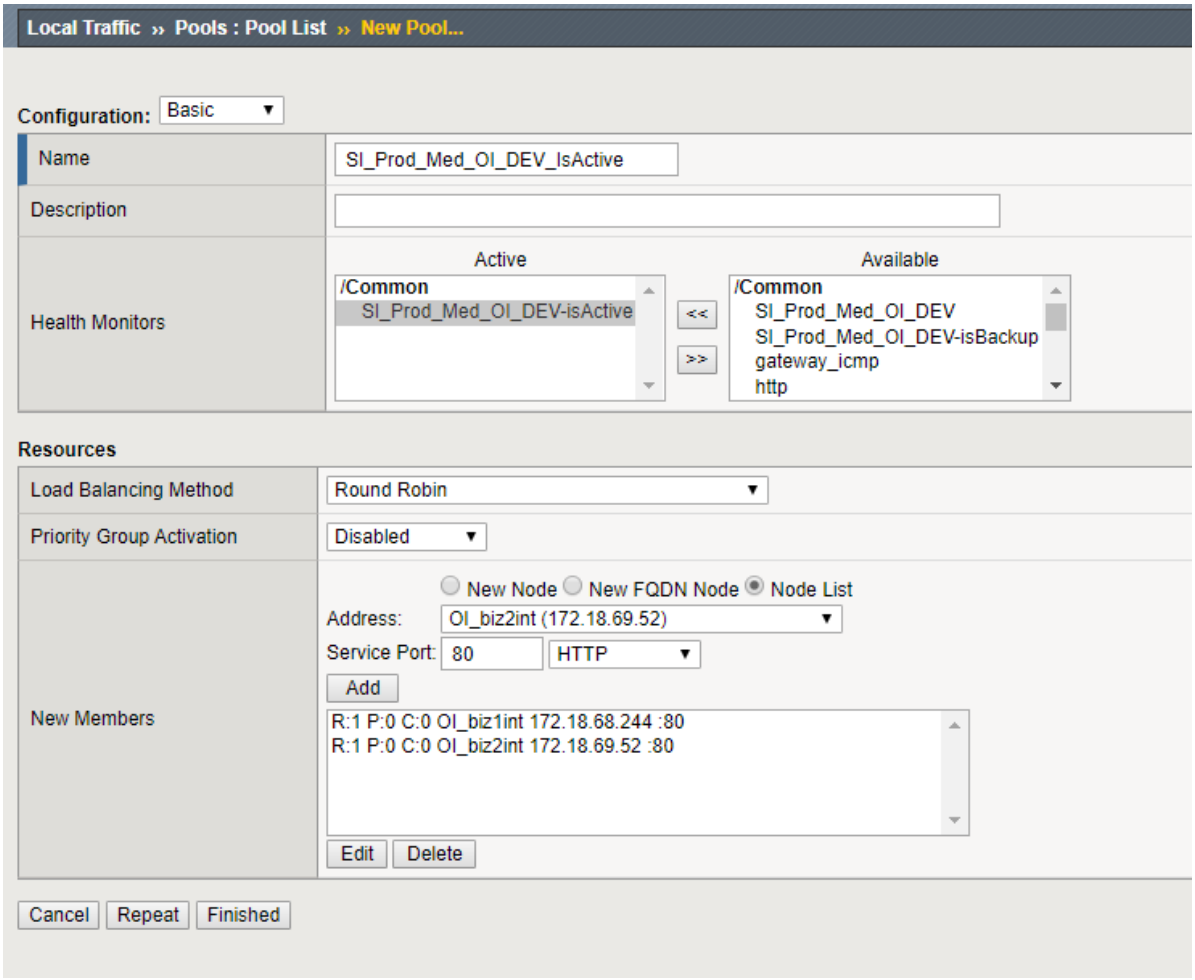

Figure 6.3 – F5 LB Configuration: Creation of new pool.

6.2.4. Virtual Servers

A virtual server is a traffic-management object on the BIG-IP system that is represented by an IP address and a service. Clients on an external network can send application traffic to a virtual server, which then directs the traffic according to your configuration instructions. The main purpose of a virtual server is to balance traffic load across a pool of servers on an internal network. Visual representation is presented on Figure 6.4 and Figure 6.5.

6.2.4.1. Create HTTP Virtual Server

1. On the Main tab, click **Local Traffic > Virtual Servers → Virtual Server List**.
2. Click **Create**.
3. In the **Name** field, type a name for virtual server (Figure 6.4).

4. In the **Type** field, select Standard.
5. In the **Source Address** field, type 0.0.0.0/0.
6. In the **Destination Address/Mask** field, type free IP address from address range for that VLAN.
7. In the **Service Port** field, select HTTP.

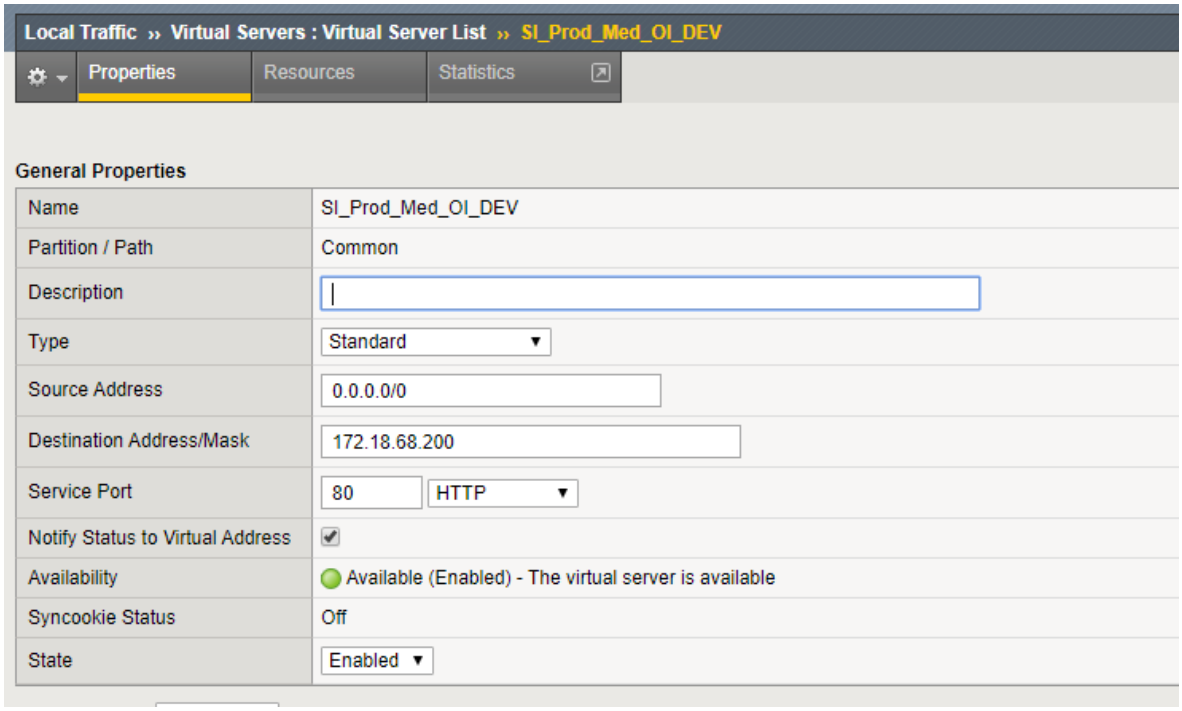

Figure 6.4 – F5 LB Configuration: Creation of virtual server – general properties

1. In the **Protocol** field, select TCP (Figure 6.5).
2. In the **Protocol profile (Client)** field, select TCP.
3. In the **Protocol profile (Server)** field, select Use Client Profile.
4. In the **HTTP Profile** field, select http.
5. In the **VLAN and Tunnel Traffic** field, select Enabled on.
6. In the **VLANs and Tunnels field**, select Internal-VLAN.
7. In the **Source Address Translation** field, select Auto Map.

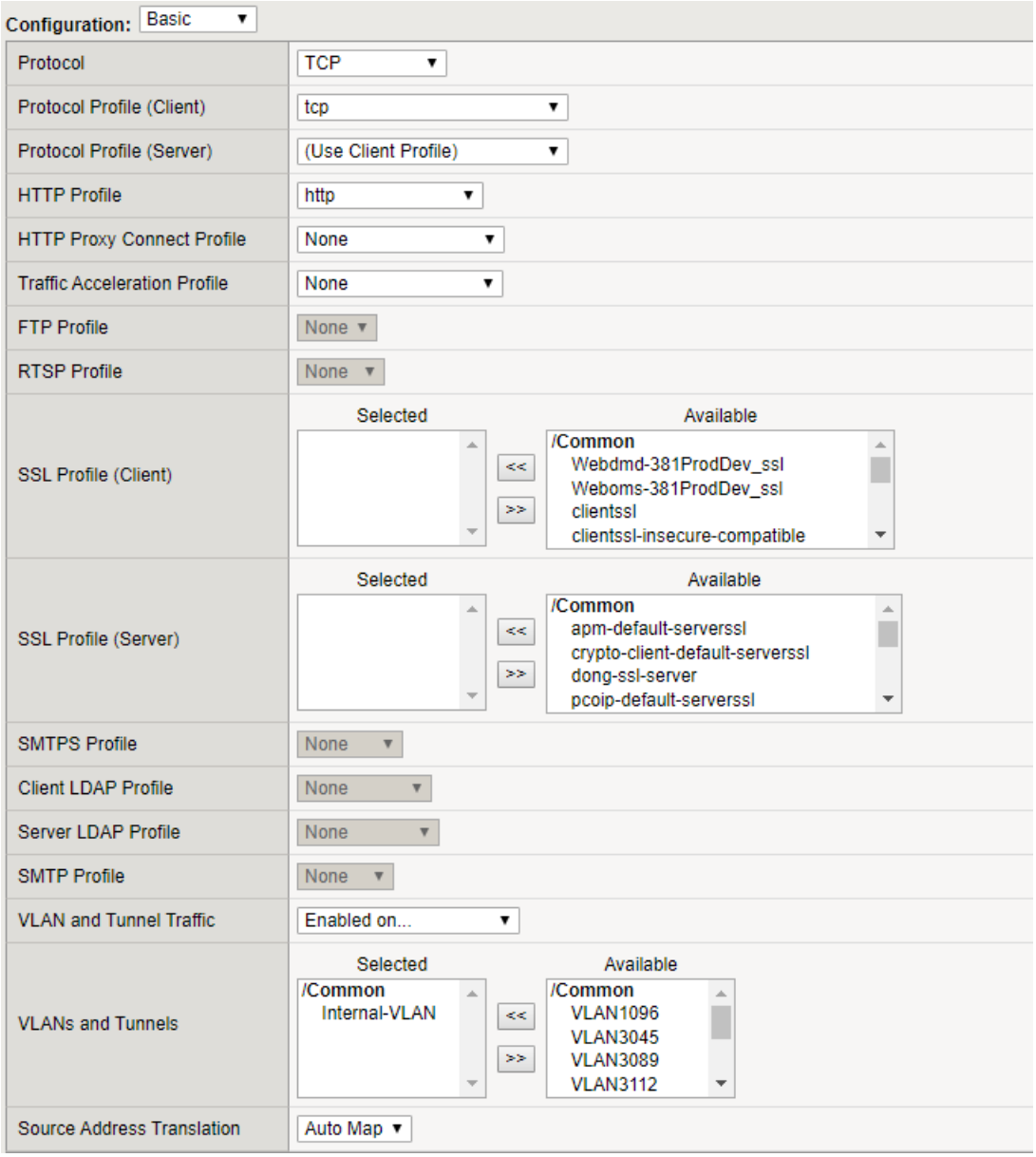

Figure 6.5 – F5 LB Configuration: Creation of virtual server – configuration

7. RELEASE NOTES

The following new features related to the SiteSwitch Interface were introduced in the software, starting from version 3.8 SP1.

8. DEFINITIONS AND ABBREVIATIONS

Definition/Abbreviation	Description
ADMS	Advanced Distribution Management System
DMZ	Demilitarized Zone
DNS	Domain Name Server
ESB	Enterprise Service Bus
NLB	Network Load Balancer
NMC	Network Management Console
REST	Representational State Transfer
SSS	Seamless Site Switch