NOKIA

NSP
Network Services Platform
Release 21.9

Service Fulfillment Application Help

3HE-17332-AAAC-TQZZA

Issue 1

September 2021

Legal notice

Nokia is committed to diversity and inclusion. We are continuously reviewing our customer documentation and consulting with standards bodies to ensure that terminology is inclusive and aligned with the industry. Our future customer documentation will be updated accordingly.

Contents

1 Service Fulfillment

1.1 Why use Service Fulfillment?

The Service Fulfilment application allows for service provisioning and activation across networks accessible to the NSP. Through the application itself, or through the northbound interface (RESTConf), Service Fulfillment enables users to make service requests that deploy services to the network using the NSP's mediation framework.

A library exists with a predefined set of service models (such as VPRN, EVPN, C-Line, E-LAN, E-TREE, E-Pipe and IES services) for both classic and model-mode SROS networks. These service models can be installed and utilized by the built-in, intent-based engine (NSP's Intent Manager) to provide assurance that service configuration is as planned/requested, and also easy adaptability for custom service model requests. New service models to support custom needs, or for third-party device support, can also be developed with aid of the NSP's automation practice team — or, if your deployment includes the NSP's programmability suite, self-development.

Network abstraction is used to simplify how the network appears to the IT/OSS layer and users of the Service Fulfillment application. This allows services to be defined and enhanced more quickly by presenting only the network service attributes and endpoints that are relevant to a specific customer's needs, thereby streamlining service fulfilment operations.

Service Fulfilment provides real-time, service-related inventory, including available Ports, LAGs, and Service Tunnels (SDPs). This allows users to view the availability of resources in the network before beginning the fulfilment process. Service offerings with customer-centric naming can be created by the user, thereby enabling dynamic creation of the service catalogue based on installed service models.

Service Fulfilment users have granular control over a service's entire life cycle. This allows them to define services without deploying them into the network, to plan services so that resources are reserved within NSP, to deploy services in the network that are fully synchronized with the intended configuration, or even to remove services from the network without deleting them entirely. users can also view all services that are in the various life cycle states, as well as view the real-time operational state of deployed services.

Service topology views are available within the Service Fulfillment application, but users are also provided with the ability to easily navigate to the NSP's Service Supervision application in order to view multi-layer topology maps and accomplish additional assurance tasks.

To ensure that intended service configurations are maintained in the network, users can audit individual services in order to view and correct any deviations, thereby ensuring configuration assurance in addition to operational assurance.

Automation is achieved using the integrated Workflow Manager application. During a service's life cycle, a workflow can be invoked to carry our specific tasks. For example, when planning a service a workflow could be invoked prior to deployment that would pre-configure policies into the network. Alternatively, when removing a service from the network, a workflow could be invoked to ensure that OAM tests and/or telemetry subscriptions are paused. Automation of user-focused workflows can also be invoked through the application itself, or via API on an ad-hoc basis against the services.

1.2 Service Fulfillment API support

Service Fulfillment functions are available for OSS using programmable APIs. For general information about developer support, visit the Nokia Network Developer Portal. For API documentation, visit the API documentation page.

For specific documentation about REST APIs for Service Fulfillment, click on API Reference in the Service Fulfillment and Resource Control > Carrier SDN row.

1.3 Intent Manager and Service Fulfillment

The Service Fulfillment application uses intent types imported from the Intent Manager application to build service templates, which are then used to build services. Users can create custom intent types within Intent Manager, as well as import predefined intent types into Intent Manager. For specific instructions, as well as information about cloning intent types, see the *NSP Intent Manager Application Help*.

Note: Intent types must have the 'ServiceFulfillment' label applied in order to be exported to the Service Fulfillment application. Users must not modify or delete any intent types with the 'ServiceFulfillment' label.

1.4 MDM adaptors and Service Fulfillment

Available application functions for model-driven NEs in Service Fulfillment can vary based on the adaptors installed. To verify the adaptors you have installed, check the Discovered Nodes list in the Device Administrator application. The Summary panel for the NE provides the list of adaptors installed for each application.

1.5 Workflow Manager and Service Fulfillment

Service Fulfillment is integrated with the Workflow Manager application. When this application is installed, Service Fulfillment can be used as a single tool to plan and automate service life cycle operations, and execute automated workflows to support service activation and enablement.

Note: A user must have Read/execute or Read/write/execute permissions within the Service Fulfillment application in order to execute workflows.

In order for workflows to be visible within Service Fulfillment, the workflow must be configured in the Workflow Manager application with the appropriate tag. These tags allow administrators to restrict workflows that are available to support service fulfillment operations without giving users access to all workflows in the Workflow Manager application. The *sf-service-operation* tag fetches service operation workflows, while the *sf-network-operation* tag fetches network operation workflows.

Using workflows can extend automated service operation capabilities in three ways:

1. Enforce input form validation rules during service create/modify operations.
2. Automatically perform pre/post deployment tasks and validations during service life cycle operations.
3. Use Workflow Execution tool to perform automated actions/tasks/workflows on existing services and network objects.

Workflows to perform the validation of input forms and perform pre/post deployment tasks are configured on a service template.

The Workflow Execution tool in Service Fulfillment allows you to select a workflow defined for service operations, input workflow parameters as required, monitor execution status, and view the input/output of execution results. You can also view past workflow executions and results for a selected service.

1.6 User access control in Service Fulfillment

Users of the Service Fulfillment application are assigned a permission level that either allows them to, or prevents them from, performing specific operations. These permissions levels are as follows, and are assigned by an NSP administrator within the User Manager application:

- None
- Read
- Read/write
- Read/execute
- Read/write/execute

Users with write permissions can perform the following operations:

- Change the state of a service
- Create an IB-SF template
- Synchronize or audit a service

Users with execute permissions can perform the following operations:

- Delete a service
- Delete an IB-SF template
- Manually invoke a workflow (the Workflow Manager application will limit the workflows that the user can invoke)

Consult the User Manager application help or your NSP administrator for more information.

1.7 What is Life Cycle State?

A service's Life Cycle State indicates the current status of the service as it transitions from the planning phase to the deployment phase and beyond. The following states may be observed:

- **Saved**
  During the service creation process, a user can save their initial configurations within the Service Fulfillment application (no associated intent instance is created). The service name will be reserved, and the user will be able to resume service creation when desired. Services in a Saved state can be deleted, or modified and saved again. When configuration is complete, Saved services can transition to either a Planned or Deployed state.
- **Planned**
  Newly-created services, or services in a Saved state, can transition to a Planned state. In this state, an associated intent instance is created in the Intent Manager application, but the service is not deployed to the network. While in a Planned state, the service's resources as reserved,

and therefore cannot be used by any other service. Services in a Planned state can be deleted (in addition to deleting the service from Service Fulfillment, this also deletes the intent instance and removes the resource reservations), or modified and kept in a Planned state. When configuration is complete, Planned services can transition to a Deployed state.

- **Deployed**
  Services in a Planned state can transition to a Deployed State. In this state, the desired configuration is sent down to the network and synchronized. Services in a Deployed state must transition to a Removed state before being deleted. If a Deployed service is modified, it will no longer be aligned with the associated intent instance. At this point, the user can either save their changes (which will place the service in the Deployed-Modified state until network synchronization occurs), or redeploy the service (which keeps the service in the Deployed state by triggering network synchronization).
- **Deployed-modified**
  Services in a Deployed-modified state have been modified by the user, but are not synchronized to the network. Services in a Deployed-modified state must transition to a Removed state before being deleted. Deployed-modified services can be further modified and saved again, (which keeps the service in the Deployed-Modified state until network synchronization occurs), or redeployed (which transitions the service to the Deployed state by triggering network synchronization).
- **Removed**
  Services in a Removed state can be deleted. In this state, the service is removed from the network, but its resources remain reserved and its associated intent instance continues to exist. Removed services can be deployed/redeployed (which transitions the service to the Deployed state) or modified and saved (which keeps the service in the Removed state).

1.8 How do I navigate the Service Fulfillment application?

The Service Fulfillment application consists of the following three pages. You can navigate from one page to another by clicking on the named tabs.

1.8.1 SERVICES page

The SERVICES page displays a list of all existing services. Additional services can be created by clicking **+ CREATE** in the top right corner.

Clicking **More** ⋮ in-line with any service presents the following options:

- Edit
- Execute Workflow
- Service details
  - Components
  - Map
  - Workflow executions
  - Lifecycle history
- Open in Service Supervision

If the service was created using the Service Fulfillment application, rather than an integrated network management system (such as NFM-P), the following additional options will be presented:

- Audit
- Synchronize

Depending on the Life Cycle State of the service, one or more of the following additional options will be presented:

- Plan
- Deploy
- Remove
- Delete

1.8.2 INVENTORY page

The INVENTORY page displays a list of all existing ports, LAGs, service tunnels, L2 service endpoints, or L3 service endpoints (depending on your selection from the drop-down menu).

When Ports are selected, click **More** ⋮ in-line with any port and choose Services Using Port to view a list of the services that are using the selected port.

When Service Tunnels are selected, click **Edit** in-line with any service tunnel to open the Update Tunnel form.

1.8.3 TEMPLATES page

The TEMPLATES page displays a list of all existing service templates or steering parameters (depending on your selection from the drop-down menu). Additional service templates and steering parameters can be created by clicking **+ CREATE** in the top right corner.

When Service Templates are selected, clicking **More** ⋮ in-line with any service template presents the following options:

- Edit
- Services Using Template
- Delete

1.9 How do I manage the display of listed information?

You can configure and save display preferences for the columns on any page of the Service Fulfillment application, as follows. Your preferences are saved for the next session.

- rearrange the sequence of columns
- re-size columns
- pin columns to the left or right of your display
- auto-size individual columns or all columns to fit data
- sort column lists based on selected attributes

  NOTE: Column sorting changes are not saved for the next session.
- show/hide columns
- export column data to CSV, XLSX, or XML

1

Open a page. The columns specific to the service, service component, or inventory object are displayed.

2

Configure the following column display preferences. To reset the columns to the settings at the start of the session, hover over the column heading and choose , then Reset Columns. To see more columns, scroll to the right.

a. Rearrange the left-to-right sequence of columns. Click and drag on a column heading.

b. Resize columns. Hover over the vertical line between two columns, then click and drag when the arrows appear.

c. Pin columns. Hover over the column heading and choose , then Pin Column: Pin Left/ Pin Right/No Pin.

d. Auto-size one or more columns to fit data. Hover over the column heading(s) and choose , then Autosize This Column or Autosize All Columns. You can also use **More** to autosize all columns.

e. Sort list objects in ascending or descending order. Click on a column header to sort the data. You can perform multi-column sorting by holding down the SHIFT key while clicking the column header. The sort icon is only visible for columns that are already sorted.

f. Clear column sorting or filters. Click **More** to the right of the column headings and choose Clear Sorting or Clear Filters.

g. Show/hide columns. Click **More** to the right of the column headings and choose Manage Columns. Deselect the columns you want to hide, or select the columns you want to show. Click APPLY.

h. Export column data to CSV, XLSX, or XML. Click **More** to the right of the column headings and choose Export to CSV, Excel export (.xlsx), or Excel export (.xml).

Note: When this action is performed, only the data loaded into memory will be exported. Additional data from the database will be excluded.

End of steps

1.10 How do I execute a service operation workflow?

Service operation workflows are tagged with *sf-service-operation*. This tag fetches service workflows from the Workflow Manager application. A service operation workflow allows you to perform automated tasks against an individual service.

1

From the SERVICES page, click **More** in-line with any service and choose Execute Workflow.

The Workflow Execution form opens.

2

Choose a workflow from the Select a workflow drop-down list.

A request is sent to the Workflow Manager application to get a list of all workflows that have been tagged with *sf-service-operation*.

3

Configure the input parameters, as required.

The inputs are predefined by the user in the workflow's Input Form in the Workflow Manager application.

You can adjust the width of the input rows using the react schema form.

4

Click **EXECUTE** to execute the workflow.

The execution status is displayed.

5

Click **VIEW RESULTS** to view the input/output data from the executed workflow.

6

Click **CLOSE**.

END OF STEPS

1.11 How do I execute a network operation workflow?

Network operation workflows are tagged with *sf-network-operation*. This tag fetches network workflows from the Workflow Manager application. A network operation workflow allows you to perform generic tasks, such as the provisioning of ports or interfaces, and checking device or network health.

1

From the SERVICES page, click **More** ⋮ in the top right corner and choose Execute Workflow.

The Workflow Execution form opens.

2

Choose a workflow from the Select a workflow drop-down list.

A request is sent to the Workflow Manager application to get a list of all workflows that have been tagged with *sf-network-operation.*

3

Configure the input parameters, as required.

The inputs are predefined by the user in the workflow's Input Form in the Workflow Manager application.

You can adjust the width of the input rows using the react schema form.

4

Click **EXECUTE.**

The execution status is displayed.

5

Click **VIEW RESULTS** to view the input/output data from the executed workflow.

6

Click **CLOSE**.

END OF STEPS

1.12 How do I view workflow executions?

Use this procedure to view the workflows that were previously executed against any service.

1

From the SERVICES page, click **More** ⋮ in-line with any service and choose View Workflow Executions.

A list of Executed Workflows is displayed.

2

Click **View Input/Output** in-line with any executed workflow.

The Quick View form opens, displaying input/output data.

Workflow execution information is stored for 90 days.

3

Click **CLOSE**.

END OF STEPS

1.13 How do I export an intent type into Service Fulfillment?

1

From the Intent Manager application, select Intent Types from the drop-down menu.

A list of intent types is displayed.

2

Click **More** ⋮ in-line with any intent type that has the ServiceFulfillment label applied and choose Export to SF from the contextual menu.

The intent type is exported to the Service Fulfillment application.

End of steps

1.14 How do I create a service template?

1

Perform 1.13 “How do I export an intent type into Service Fulfillment?” (p. 12).

2

From the TEMPLATES page, select Service Polices from the drop-down menu and click **+ CREATE**.

The Create a service template form opens.

3

Configure the parameters, as required.

Parameter	Description
Template Name	Specifies the name of the template
Description	Describes the template
Intent type	Specifies the intent type to associate with the template
Intent version	Specifies which version of the selected intent type to associated with the template
State	Specifies the state of the template, Released or Draft
UI Config	Specifies the interface to be used with the template

4

If required, click **+ ADD** in the Workflows panel to add workflows to the service template.

The Add Workflows form opens.

5

Configure the parameters, as required:

Parameter	Description
Workflow Name	Specifies the workflow to be executed
Service Life Cycle State	Specifies the life cycle state of the service that will trigger workflow execution

Parameter	Description
Service Life Cycle Case	Specifies the case, Success or Fail, relative to the life cycle state that will trigger workflow execution
Blocking	Specifies whether unsuccessful execution of the workflow will prevent service life cycle state changes
Workflow Execution Timeout (seconds)	Specifies the length of time, in seconds, that unsuccessful execution of the workflow will prevent service life cycle state changes

6

Click **ADD**.

The Add Workflows form closes and the workflow is added to the service template.

7

Click **CREATE**.

The service template is created.

END OF STEPS

1.15 What are E-Pipe services?

An E-Pipe service connects two customer Ethernet ports over a WAN. Service Fulfillment supports the creation of E-Pipe services over IP networks. When an E-Pipe service is deployed, the selection of the endpoints utilizes automatically the requisite technology tunnels. For example, when the tunneling technology is MPLS, a service tunnel with a single LSP satisfying the service-specified constraints and objectives is automatically selected. The service is then bound to that LSP via the service tunnel. NSP tracks the LSP available bandwidth and adjusts it automatically to accommodate the E-Pipe service, which reserves bandwidth on the LSP.

If an existing E-Pipe service is modified (for example, to increase bandwidth), the service tunnel is resized to accommodate it, if permitted by policy. If the service tunnel resizing fails, the service tunnel may be rerouted onto links that cannot accommodate the resized service tunnel. If the reroute fails, then a new service tunnel is created. It is possible for E-Pipe services to use service tunnels that were not created using Service Fulfillment.

Note: Policies for service-to-tunnel binding dictate the rules associated with the service binding. If no service tunnel meets all the constraints, and this is a new E-Pipe service, a new service tunnel is created.

Other parameters of the E-Pipe service are obtained from the specific templates referenced in the abstract API definition. The service definition in the abstract API, the detailed configuration in the service templates, and other network and tunnel parameters form the complete service definition, which is represented in the normalized model for E-Pipe. Specific configurations based on the devices are then constructed and deployed using the NFM-P.

Note: You can provision SAP-to-SAP E-Pipe services if you select different ports for each endpoint.

1.15.1 What are brownfield E-Pipe services?

The E-Pipe services created within the NFM-P (brownfield E-Pipe services) can be managed by Service Fulfillment. In order for Service Fulfillment to discover these services, their “NSD-managed” flag must be enabled within the NFM-P. Once discovered by Service Fulfillment, these services will function the same as E-Pipe services created within Service Fulfillment itself, provided that they meet NSP requirements. Any change made to these services within NFM-P after discovery will be propagated to Service Fulfillment, provided the change impacts the topology of the service.

Note: E-Pipe services created within the NFM-P have an “Auto-delete” flag. When enabled, services without service sites are automatically deleted. This flag should not be enabled on services being managed by Service Fulfillment, as the “NSD-managed” flag is disabled upon service deletion, and remains so even if the service is recreated and resynchronized into Service Fulfillment.

1.15.2 What are EVPN-based E-Pipe services?

Service Fulfillment supports the creation of EVPN-based E-Pipe services over tunnel types that are supported in a BGP-EVPN MPLS context. The EVPN-based E-Pipe service is not established over pseudowire. You can configure EVPN-based E-Pipe services on all the Nokia NEs that support EVPN. The configuration of EVPN-based E-Pipe services on multi-vendor NEs is not supported.

To configure an EVPN-based E-Pipe service, you need to start the E-Pipe service creation in Service Fulfillment application, as usual, and select the Enable EVPN Tunnel Selection check box in the Additional Properties form. After enabling the EVPN service, you are able to select a tunnel type from the following options: LDP, RSVP-TE, SR-ISIS, SR-OSPF, SR-TE, and BGP. There is also the ANY option, which indicates to the NEs that any supported tunnel type in the EVPN context can be selected following the order of preference.

The following considerations apply to the EVPN-based E-Pipe service configuration in Service Fulfillment:

- Service Fulfillment supports only the configuration of greenfield EVPN-based E-Pipe service. The modification of existing EVPN-based E-Pipe services that were created in the NFM-P is not supported.
- Service Fulfillment assumes that the network is correctly configured to support the selected tunnel type. The service can fail if the network is not correctly configured. For example, if the network does not have SR-TE LSPs configured, then an EVPN-based E-Pipe service configured with the SR-TE tunnel type is operationally down.
- The tunnel type parameter is modifiable, as required. However, Service Fulfillment does not support switching from the EVPN-based E-Pipe (the Enable EVPN Tunnel Selection check box is selected) to a pseudowire-based E-Pipe (the Enable EVPN Tunnel Selection check box is not selected).
- Each service is associated with a unique EVPN instance (EVI) number that Service Fulfillment generates automatically and then sends to the NE to auto-derive the unique RD/RT for the NE. Service Fulfillment synchronizes the EVIs defined in the network to ensure the EVI uniqueness.
- The EVPN-based E-Pipe service uses an Ethernet Tag (eth-tag) that is pre-configured by NSP

and not visible in the GUI. The NE uses the Ethernet Tag to identify its remote BGP peer and establish the MP-BGP connection.

To ensure consistency when configuring multiple similar services, you can create EVPN-based E-Pipe service templates that you can then apply to your service. Select the appropriate Tunnel Type for EVPN-based E-Pipe in the template properties, as required.

1.16 How do I create an E-Pipe service?

Use this procedure to create an E-pipe service. The parameters that are available to you is dependant on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided E-pipe template is being used.

1

Perform 1.14 “How do I create a service template?” (p. 13).

2

From the SERVICES page, click **+ CREATE**.

The Select service template to start form opens displaying a list of service templates.

3

Click on an E-pipe service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service
Customer ID	Specifies the customer ID
NE Service ID	Specifies the NE service ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number
MTU	Specifies the service MTU

5

In the Site A panel, specify the Device ID, then click **+ ADD**.

The Add Endpoint form opens.

6

Configure the parameters, as required:

Parameter	Description
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP

7

In both the ingress and egress panels, configure the parameters as required:

Parameter	Description
Queue Group Redirect List	Specifies the assigned queue group redirect list
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier for the policer

Parameter	Description
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **ADD** to add the endpoint. The Add Endpoint form closes.

8

Configure the PW Switching parameters, as required:

Parameter	Description
Primary Hub ID	Specifies the identifier of the primary hub
Secondary Hub ID	Specifies the identifier of the secondary hub

9

In the Site B panel, specify the Device ID, then click **+ ADD**.

The Add Endpoint form opens.

10

Repeat Step 6 to Step 8 for Site B.

11

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

12

Configure the parameters, as required:

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by Service Fulfillment
SDP ID	Specifies the SDP identifier xPath
VC ID	Specifies the SDP virtual circuit identifier
Description	Describes the SDP binding
Admin State	Specifies the desired state of the service SDP binding

Click **ADD** to add the SDP binding. The Add SDP form closes.

13

Perform one of the following:

a. Enable the Reserve Resources checkbox and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.7 “What is Life Cycle State?” (p. 7) for more information.

END OF STEPS

1.17 What are E-Access services?

NSP supports the creation of E-Pipe services between an NE that is managed by an NSP instance and an NE that is located in a different domain and managed by a different NSP instance or by a third-party system. This applies to cases in which your NSP does not manage the entire network. This type of service is called an E-Access service. An E-access service is only supported on NFM-P managed NEs. NSP supports the creation of an E-Access service only by way of the NSP REST API. To create an E-Access service, use the POST /api/v4/services/eaccess operation, Create an IP E-Access service.

For the E-Access service creation to work, you must use an SDP tunnel, a path and an LSP that were already configured on each NE between the two NEs. You also need to configure a Tunnel Selection policy to apply to the E-Access service. Select the Use existing tunnels option as the service provisioning rule.

A few pointers to help you configure an E-Access service:

- NSP books bandwidth only at the Access interface level, not on the LSP in the core.
- The service uses the VC-ID label specified on the Adjacency on the spoke-sdp binding.
- If the Service ID is not already in use, NSP assigns the VC-ID label as the Service ID. If that Service ID is already in use, NSP auto-assigns the next available ID.
- If you specify a VC-Type label, then it must match the VC-Type defined at the far end. The default value is Ethernet_Tagged_Mode, which maps to VLAN on the NE.
- E-Pipe service templates can be applied to E-Access services.

After creating the E-Access service, you can view the service and its properties in Service Fulfillment.

- The Service layer shows just the NE, along with the service endpoint, that is in the network managed by your NSP.
- The Service Tunnel layer shows the Service Tunnel connection. This is the existing SDP that you created for the service.
- The MPLS layer shows the LSP. This is the existing LSP that you created for the service.
- The service does not show an IGP layer because your NSP does not manage the far-end NE and therefore is not aware of the IGP path.
- The service does not show a physical layer because your NSP does not manage the far-end NE.

1.18 What are VPRN services?

Service Fulfillment supports the creation of VPRN services. VPRN services utilize layer 3 VRF (VPN/virtual routing and forwarding) to routing tables for each customer utilizing the service. The customer peers with the service provider router and the two exchange routes, which are placed into a routing table specific to the customer. Multiprotocol BGP (MP-BGP) is required to utilize the service.

The RD and RT is auto-generated as per policy direction and the topology type selected. Parameters specified in the referenced template complete the service definition. Other parameters of the VPRN service are obtained from the specific templates referenced in the abstract API definition. The service definition in the abstract API, the detailed configuration in the service templates, and other network and tunnel parameters form the complete service definition, which is represented in the normalized model for VPRN. Specific configurations based on the devices are then constructed and deployed using NFM-P. VPRN services can use service tunnels that were not created using Service Fulfillment.

The discovery and deployment of a hub-and-spoke VPRN service where two hubs are configured for redundancy is supported on NFM-P and MDM managed NEs. Redundancy is achieved by having the hubs advertise the same import/export routes with a unique route distinguisher. This feature is not supported on Wavence SM NEs.

Service Fulfillment allows you to configure the properties on each hub-and-spoke or full mesh VPRN service site. You can also configure one or more SAPs on an VPRN service site.

Note: Before provisioning VPRN services using NSP, you must have MP-BGP configured and working between the PE nodes to support IP VPN. The Peer CE nodes must also be configured. Only one AS is supported per provider.

1.19 How do I create a VPRN service?

Use this procedure to create an VPRN service. The parameters that are available to you is dependant on the intent type that is associated with the service template you select, and may differ from those described in this procedure, which assumes the Nokia-provided VPRN template is being used.

1

Perform 1.14 “How do I create a service template?” (p. 13).

2

From the SERVICES page, click **+ CREATE**.

The Select service template to start form opens displaying a list of service templates.

3

Click on a VPRN service template from the list.

The Create Service form opens with the Template Name parameter populated.

4

Configure the parameters, as required:

Parameter	Description
Service Name	Specifies the name of the service
Customer ID	Specifies the customer ID
NE Service ID	Specifies the NE service ID
Description	Describes the service
Admin State	Specifies the initial administrative state of the service upon deployment
Job ID	Specifies the work-order number

5

In the Site Details panel, click **+ ADD**.

The Add Site form opens.

6

Configure the parameters, as required:

Parameter	Description
Device ID	Specifies the assigned queue group redirect list
VRF Name	Specifies the name of the VRF
Autonomous System	Specifies the AS number advertised to peers for this router
Enable OSPF	Specifies whether OSPF protocol is enabled
Route Distinguisher Type	Specifies the route distinguisher type
Route Distinguisher	Specifies the route distinguisher
VRF Import	Specifies the name of the VRF import policy
VRF Export	Specifies the name of the VRF export policy
Description	Describes the VRF
Route Target (click **+ ADD**)	
Target Type	Specifies the type of route target
Target Value	Specifies the route target value
Autobind Tunnel	
Resolution	Specifies the MBS of the queue
Enforce Strict Tunnel Tagging	Specifies the PIR rate of the queue
Resolution Filter	
BGP	Specifies the BGP type for the autobind tunnel
GRE	Specifies whether GRE is enabled for the autobind tunnel
LDP	Specifies whether LDP is enabled for the autobind tunnel
RSVP	Specifies whether RSVP is enabled for the autobind tunnel
SR ISIS	Specifies whether SR ISIS is enabled for the autobind tunnel
SR OSPF	Specifies whether SR OSPF is enabled for the autobind tunnel

Parameter	Description
SR-TE	Specifies whether SR-TE is enabled for the autobind tunnel
UDP	Specifies the UDP type for the autobind tunnel
RIB API	Specifies whether RIB API is enabled for the autobind tunnel
MPLS Fwd Policy	Specifies whether MPLS Fwd policy is enabled for the autobind tunnel
SR Policy	Specifies whether SR policy is enabled for the autobind tunnel
SR OSPF3	Specifies whether segment routing OSPF3 is used for next hop resolution
Maximum IPv4 Routes	
Max Number of Routes	Specifies the maximum number of IPv4 routes that are configured on the virtual router
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv4 routes that the VRF holds
Log Only	Specifies whether action is taken when the maximum number of IPv4 routes, held within a VRF context, is reached
Maximum IPv6 Routes	
Max Number of Routes	Specifies the maximum number of IPv6 routes that are configured on the virtual router
Mid Route Threshold	Specifies the mid-level water marker for the number of IPv6 routes that the VRF holds
Log Only	Specifies whether action is taken when the maximum number of IPv6 routes, held within a VRF context, is reached
Mc Maximum Routes	
Max Number of MCast Routes	Specifies the maximum number of multicast routes that are configured on the virtual router
Mid Route MCast Threshold	Specifies the mid-level water marker for the number of multicast routes that the VRF holds

Parameter	Description
Log Only	Specifies whether action is taken when the maximum number of multicast routes, held within a VRF context, is reached
eBGP Details	
Loop Detect	Specifies the strategy for loop detection in the AS path
Next Hop Resolution	Specifies whether BGP routes can be used to resolve BGP nexthop
Best Path Selection	
Compare Origin Validation State	Specifies whether the origin validation state is used in the BGP decision process
Deterministic MED	Specifies whether paths will be grouped based on AS before MED attribute comparison
Origin Invalid Unusable	Specifies whether routes that have an origin validation state of 'Invalid' can be used
Ignore NH Metric	Specifies whether next-hop distance will be ignored during best path selection
Always Compare MED	
MED Value	Specifies the Always Compare MED context
Strict AS	Specifies whether MED attributes will be compared from same-neighbor AS routes only
AS Path Ignore	
IPv4	Specifies whether AS path length will be ignored for unlabeled unicast IPv4 routes
IPv6	Specifies whether AS path length will be ignored for unlabeled unicast IPv6 routes
Label IPv4	Specifies whether AS path length will be ignored for labeled unicast IPv4 routes
Ignore Router ID	Specifies the ignore-router-id context
Ebgp Ibgp Equal	
IPv4	Specifies whether to consider EBGP and IBGP labeled IPv4 routes equal
IPv6	Specifies whether to consider EBGP and IBGP labeled IPv6 routes equal

Parameter	Description
Label IPv4	Specifies whether to consider EBGP and IBGP unlabeled IPv4 routes equal
Group (**+ ADD**)	
Group Name	Specifies the group name
Damping	Specifies whether BGP route damping is used to reduce route flap
Authentication Key	Specifies the BGP authentication key for all peers
Peer AS	Specifies the peer AS number
Peer IP Tracking	Specifies whether BGP peer tracking is enabled
Neighbor (**+ ADD**)	
Import Policy	Specifies the import policy name
Export Policy	Specifies the export policy name
IP Address	Specifies the IP address that the neighbor uses to communicate with BGP peers
Group Name	Specifies the group name
Peer AS	Specifies the peer AS number
Admin State	Specifies the administrative state of the BGP neighbor
Split Horizon	Specifies whether to prevent routes being reflected back to best-route peer
Authentication Key	Specifies the BGP authentication key for peer
Description	Describes the BGP neighbor
AS Override	Specifies whether the peer's ASN will be replaced by the local ASN in AS Path

7

In the Interface Details panel, click **+ ADD**.

The Add Interface form opens.

8

Configure the parameters, as required:

Parameter	Description
Interface Name	Specifies the name of the interface
Description	Describes the interface
Administrative State	Specifies the administrative state of the interface
Loopback	Specifies whether to use the interface as a loopback interface
IP MTU	Specifies the interface IP MTU
Primary	
Address	Specifies the primary IPv4 address assigned to the interface
Prefix Length	Specifies the primary IPv4 address prefix length
Secondary (**+ ADD**)	
Address	Specifies the secondary IPv4 address assigned to the interface
Prefix Length	Specifies the secondary IPv4 address prefix length
VRRP (**+ ADD**)	
Virtual Router ID	Specifies the virtual router identifier for the VRRP virtual router instance
Backup	Specifies virtual router IP addresses for the interface
Priority	Specifies the base priority for the VRRP
SAP	
Port ID	Specifies the port identifier
Inner VLAN Tag	Specifies the inner VLAN tag
Outer VLAN Tag	Specifies the outer VLAN tag
Admin State	Specifies the administrative state of the service
Description	Describes the SAP
IPv6 (**+ ADD**)	

Parameter	Description
IPv6 Address	Specifies the IPv6 address assigned to the interface
Prefix Length	Specifies the IPv6 address prefix length
OSPF	
Area ID	Specifies the area identifier
Interface Type	Specifies the interface type to broadcast or point-to-point
Passive	Specifies whether to allow the interface to be advertised as an OSPF interface without running the OSPF protocol
Admin State	Specifies the administrative state of the OSPF interface

9

In the SAP panel, configure the following parameters for both ingress and egress, as required:

Parameter	Description
Queue Group Redirect List	Specifies the assigned queue group redirect list
QoS	
Match QinQ Dot1p (ingress only)	Specifies the match QinQ Dot1p
QinQ Mark Top Only (egress only)	Specifies whether top Q-tags are marked
SAP Ingress	
Policy Name	Specifies the name of the ingress SAP policy
Queuing Type	Specifies the ingress queuing type
SAP Egress	
Policy Name	Specifies the name of the egress SAP policy
Queue (click **+ ADD**)	
Queue ID	Specifies the unique identifier for the queue
CBS	Specifies the CBS of the queue
MBS	Specifies the MBS of the queue
PIR	Specifies the PIR rate of the queue
CIR	Specifies the CIR rate of the queue

Parameter	Description
Policer (click **+ ADD**)	
Policer ID	Specifies the unique identifier for the policer
CBS	Specifies the CBS of the policer
MBS	Specifies the MBS of the policer
Policer Control Policy	
Policy Name	Specifies the name of the policer control policy
Scheduler Policy	
Policy Name	Specifies the name of the scheduler policy
Scheduler (click **+ ADD**)	
Scheduler Name	Specifies the name of the scheduler
PIR	Specifies the PIR rate of the scheduler
CIR	Specifies the CIR rate of the scheduler
Filter	
IP	Specifies the IP filter identifier
IPv6	Specifies the IPv6 filter identifier

Click **ADD** to add the interface. The Add Interface form closes.

10

In the Static Route Details panel, click **+ ADD**.

The Add Static Route form opens.

11

Configure the parameters, as required.

Parameter	Description
IP Prefix	Specifies the IP prefix for the static route
Prefix Length	Specifies the prefix length for the static route
Is Blackhole	Specifies whether the prefix is a blackhole route
Next Hop (**+ ADD**)	
IP Address	Specifies the IP address of the next hop

Parameter	Description
Preference	Specifies the priority of this static route over routes from different sources
Admin State	Specifies the administrative state of next hop
Indirect (**+ ADD**)	
IP Address	Specifies the IP address of the next hop
Preference	Specifies the priority of this static route over routes from different sources
Admin State	Specifies the administrative state of next hop

Click **ADD** to add the static route. The Add Static Route form closes.

12

Click **ADD** to add the endpoint.

The Add Endpoint form closes.

13

In the SDP Details panel, click **+ ADD**.

The Add SDP form opens.

14

Configure the parameters, as required:

Parameter	Description
Source Device ID	Specifies the SDP source device identifier
Destination Device ID	Specifies the SDP destination device identifier
Steering Parameter	Specifies the steering parameter used by Service Fulfillment
SDP ID	Specifies the SDP identifier xPath
VC ID	Specifies the SDP virtual circuit identifier
Description	Describes the SDP binding
Admin State	Specifies the desired state of the service SDP binding

Click **ADD** to add the SDP binding. The Add SDP form closes.

15

Perform one of the following:

a. Enable the Reserve Resources checkbox and click **PLAN** to create the service in a Planned state.

b. Click **SAVE** to create the service in a Saved state.

c. Click **DEPLOY** to create the service in a Deployed state.

See 1.7 “What is Life Cycle State?” (p. 7) for more information.

END OF STEPS

1.20 How do I audit a service?

1

From the SERVICES page, click **More** ⋮ in-line with any service and choose Audit.

The service is audited.

2

If an Audit Result form appears, one or more attributes and/or objects are misaligned. Review the results and click **OK**.

The Audit Result form closes.

3

To revert to the expected value of a misaligned attribute, or to restore a misaligned object, click **More** ⋮ in-line with the previously-audited service and choose Synchronize.

The service is synchronized with the network.

END OF STEPS

1.21 How does NSP handle brownfield LSPs and SDP tunnels?

NSP can discover LSP and SDP tunnels created previously with NFM-P, including multi-vendor LSP and SDP tunnels, with the following exceptions:

- A single SDP tunnel that uses multiple LSPs
- Multiple SDP tunnels that use the same LSP

1.21.1 Service tunnels (SDP)

NSP allows you to create services with bandwidth constraints on service tunnels created previously with NFM-P. NSP operates with initial allocated bandwidth on these tunnels and keeps track of used bandwidth for all created services. It is assumed that NSP is the only entity creating services on these tunnels. NSP can delete or resize the allocated bandwidth, as well as modify the LSPs associated with service tunnels previously created with NFM-P.

1.22 Can I create services on SDPs with multiple loopback IP addresses?

NSP supports the configuration of services on SDP tunnels using a loopback IP address as either the source or destination IP address when routing services. A potential benefit of having services on SDP tunnels using a loopback IP address is the ability to configure routing on tunnels established on different paths between two NEs. However, you can configure such services only on brownfield SDP tunnels that were created in NFM-P or on NEs. NSP does not support the creation of new service tunnels using loopback IP addresses.

Before you start configuring a service in NSP, you must create SDP tunnels with loopback IP addresses in NFM-P or on the NE. The following list captures the high-level configuration tasks required for each NE.

- Configure the loopback interfaces on routers.
- Configure peers on the targeted LDPs. Use the loopback interface name as the local-lsr-id option and enable tunneling to enable LDP over the tunnels.
- Configure the SDP tunnels using the loopback interface IP addresses for the service far end. Optionally, you can apply a steering parameter to the tunnel to help the selection of the correct SDP tunnel when creating the service.

The service tunnels that you created can be viewed in Service Fulfillment on the INVENTORY tab. The service tunnel Destination IP is the IP address of the loopback interface and the service Transport type is MPLS.

If you applied the optional steering parameter to the tunnel, then you can also create a tunnel selection policy for the steering parameter.

1.23 What are brownfield service tunnels?

Brownfield service tunnel are tunnels created previously in NFM-P that you can discover and then use with services created using Service Fulfillment.

You can modify the parameters of a discovered brownfield service tunnel in Service Fulfillment. This enables you to support services with bandwidth booking in the core and to restrict or to allow for consumption, modification and deletion in a different way from how the service tunnels were discovered.

1.24 How do I enable NSP management on services created using the NFM-P?

1

Choose **Manage→Service→Services** from the NFM-P main menu. The **Manage Services** form opens.

2

Click **Search** and choose a service.

The following table maps the service names defined in the NFM-P to the corresponding NSP service names.

NFM-P service	NSP service
CPIPE	C-LINE
EPIPE	E-Pipe
VPLS	E-LAN
VPRN	VPRN

3

Enable the check box in the NSD Managed column for the selected service.

4

Save your change and close the form.

END OF STEPS

1.25 How do I augment services, sites, or endpoints?

In order to deploy IP services to NFM-P, NSP uses NFM-P templates that are installed in NFM-P during NSP installation. The use of these templates are hard-coded in NSP, however, NSP service definition is very abstract and models only a small subset of available attributes on the NEs. As a result, you cannot configure certain attributes from Service Fulfillment that would otherwise be available from the NFM-P.

The following workflow can be used to augment NSP services, sites, and endpoints such that additional attributes can be configured from Service Fulfillment.

1

Create one or more json files that define the additional attributes to be made accessible from Service Fulfillment, and store them in the NSP database. For an example of how the files should be written, see the *NSP DevOps Portal*.

2

Use the GET /v4/mediation/augmentation-meta/ API command to create an augmentation meta. The *pathName* (specifies the entity to be augmented), *templateName* (specifies the custom NFM-P system script that will be used to interpret the additional attributes), and *augmentationMetaJsonFileName* (specifies the path to the json file) parameters must be configured. The *pathName* parameter supports only the following values:

- 'nsd-service:/services/elan-sites'
- 'nsd-service:/services/eline-sites'
- 'nsd-service:/services/l3vpn-sites'
- 'nsd-service:/services/ies-sites'

- 'nsd-service:/services/elan-sites/site'
- 'nsd-service:/services/eline-sites/site'
- 'nsd-service:/services/l3vpn-sites/site'
- 'nsd-service:/services/ies-sites/site'
- 'nsd-service-evpn:/services/elan-evpn-sites/site'
- 'nsd-service-evpn:/services/eline-evpn-sites/site'
- 'nsd-service:/services/elan-sites/site/endpoints/endpoint'
- 'nsd-service:/services/eline-sites/site/eline-groups/eline-group/port-endpoints/port-endpoint'
- 'nsd-service:/services/l3vpn-sites/site/endpoints/endpoint'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint'
- 'nsd-service-evpn:/services/elan-evpn-sites/site/endpoints/endpoint'
- 'nsd-service-evpn:/services/eline-evpn-sites/site/port-endpoints/port-endpoint'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint/static-routes/static-route'
- 'nsd-service:/services/l3vpn-sites/site/static-routes/static-route'
- 'nsd-service-ies:/ies-sites/site/endpoints/endpoint/bgp-peers/bgp-peer'
- 'nsd-service:/services/l3vpn-sites/site/bgp-peers/bgp-peer'

3

Create a custom NFM-P template to interpret the additional attributes and install into NFM-P, as follows:

- For an example of how a custom template should be written, see the default templates located at */opt/nsp/configure/nfmpTemplates/nfmpTemplates.zip*.
- Copy the *nfmpTemplates.zip* and *install_nfmpTemplates.sh* files and Chmod 777 them.
- Execute the *su samadmin -c "bash ./install_nfmpTemplates.sh"* command and wait for the nfmp log message “Script complete”.
- Verify that your custom script is returned using the GET /sdn/api/v4/template/nfmp-template API command.

4

From the Policy Management application, create a new mediation profile that includes the newly-created custom NFM-P script. See the Policy Management application help for information about configuring mediation profiles.

5

From the Policy Management application, create a new service template that includes the newly-created mediation profile. See the Policy Management application help for information about configuring service templates.

6

From the Service Fulfillment application, create a new service that uses the newly-created service template. Service Fulfillment retrieves augmentation data associated to this template

and automatically renders the defined attributes at the service, site, and endpoint levels. Service Fulfillment stores the input to these fields and invokes the custom NFM-P script defined in the service template during service creation and modification. See the Service Fulfillment application help for information about configuring services.

End of steps

1.26 How do I resynchronize augmented properties?

Once additional attributes have been made accessible to Service Fulfillment via the workflow in the *How do I augment services, sites, or endpoints?* procedure, it is possible that the attributes may be modified elsewhere (such as NFM-P), resulting in incorrect displayed values within Service Fulfillment. To rectify this, resynchronization augmentation scripts can be created and placed in tomcat's classpath as a jar archive which will be picked up when tomcat starts up. Alternatively, these scripts can be deployed into a configurable location in the filesystem.

The default location is */opt/nsp/configure/nfmpResyncAugmentationScripts/*. If scripts are available in both tomcat's classpath and a location in the filesystem, the filesystem version will be given preference. This is because the scripts in the filesystem can be modified without having to restart tomcat. To change the default location in the filesystem, add the following text to the sam-plugin section of the */opt/nsp/configure/config/arm-system.conf* file:

```
sam-plugin
{
  resync_augmentation_scripts_path="<custom_location>"
}
```

Where *custom_location* is the location where resynchronization augmentation scripts will be stored.

Resynchronization augmentation scripts should be named as follows:

```
<classname>.resync-augenmentation.js
```

Where *classname* is one of the supported NFM-P class names listed below:

- epipe.Epipe
- vpls.Vpls
- vprn.Vprn
- ies.Ies
- epipe.Site
- vpls.Site
- vprn.Site
- ies.Site
- vll.L2AccessInterface
- vpls.L2AccessInterface
- service.L3AccessInterface
- bgp.Peer

- rtr.StaticRoute

Perform the following workflow to jar the resynchronization augmentation scripts package:

1

Execute the following commands:

```
cd opt/nsp/configure/nfmpResyncAugmentationScripts
jar cvf  ./nfmp-resync-augmentation.jar ./*.resync-augmentation.js
```

2

Copy *nfmp-resync-augmentation.jar* to sdn app's lib folder. Execute:

```
cp ./nfmp-resync-augmentation.jar
/opt/nsp/server/tomcat/webapps/sdn/WEB-INF/lib/
```

3

Restart nsp-tomcat. Execute:

```
nspdctl restart
```

END OF STEPS