AppViewX

Modular Persona Based Virtual Server Creation Workflow Guide

Trademarks

Contact Information

AppViewX, Inc.

500 Yale Avenue North, Suite 100

Seattle, WA 98109

Tel: +1 (206) 207 7541

Email: info@appviewx.com

Web: www.appviewx.com

Document Information

Software Version: 12.3.0

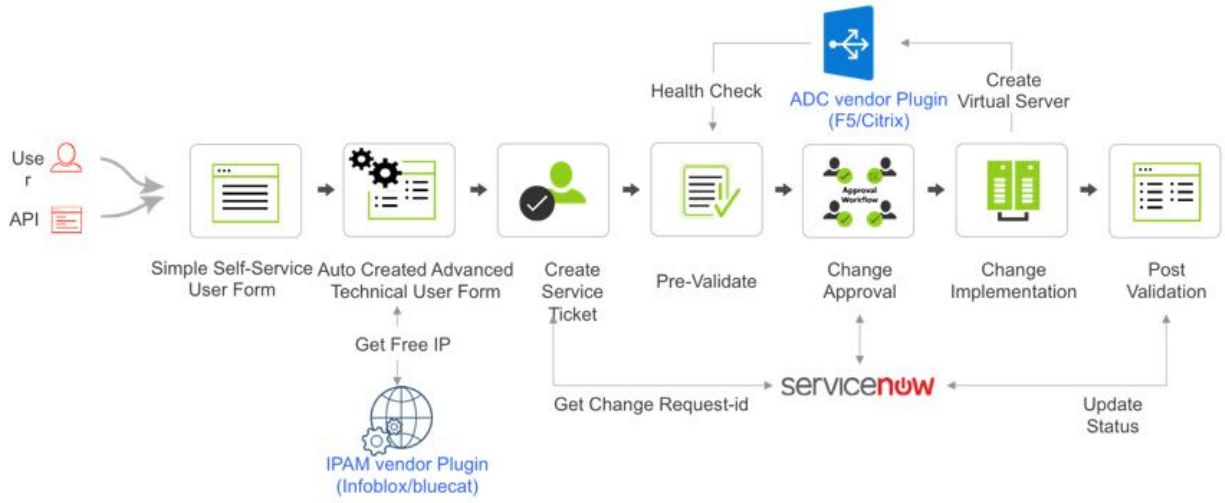
Document Version: 1.0

Last Updated on: June 01, 2018

Contents

1 Description

The Modular Persona Based Virtual Server Creation workflow is used to create a virtual server with profiles, monitors, pool, and pool members in F5 Big-IP LTM and Citrix NetScaler SLB devices. The IP Address Management (IPAM) devices like Infoblox or BlueCat can be integrated to this workflow, which allows the users to reserve a free IP address from the available address pools and create DNS binding for the new virtual server. Also, the workflow allows the users to create a change request tickets in IT Service Management (ITSM) tool called ServiceNow for approvals and tracking. The service request change ID is associated with the work order and is updated based on the implementation status.



A persona based approach enables the Application owner to capture the user's intent and provision a new application using the simple self-serviceable user form. The self-service user form abstracts the underlining network infrastructure level details from the end user and translates it to the vendor specific configuration, which is then displayed to the admin user in the advanced user form.

The admin user can perform the following using the advanced user-form:

- Select the LTM or SLB device by checking the real-time performance metrics of the available LTM(s) or SLB(s).
- Update the auto-generated configurations such as load balancing method, add a new application servers and so on.

The workflow provides modularity to change the IPAM vendor from Infoblox to BlueCat and the ADC vendor from Citrix to F5 by simply replacing the corresponding subflow in the workflow studio. A new vendor can be integrated with this workflow by creating or importing a vendor specific subflow. The same workflow can be reused with minimal changes to avoid the vendor lock-in and it has the flexibility to build over your existing automation investments.

The work order pre-validates the LTM or SLB device performance metrics (such as CPU and memory utilization) and confirms that the new virtual server and associated objects are not available. On successful pre-validation, the configuration changes are reviewed through a two-level approval process: first by ServiceNow, then by AppViewX. After approval is received, the configuration changes are implemented on the device. A post-validation script ensures the virtual server and the associated objects are created successfully on the respective device.

2 Prerequisites

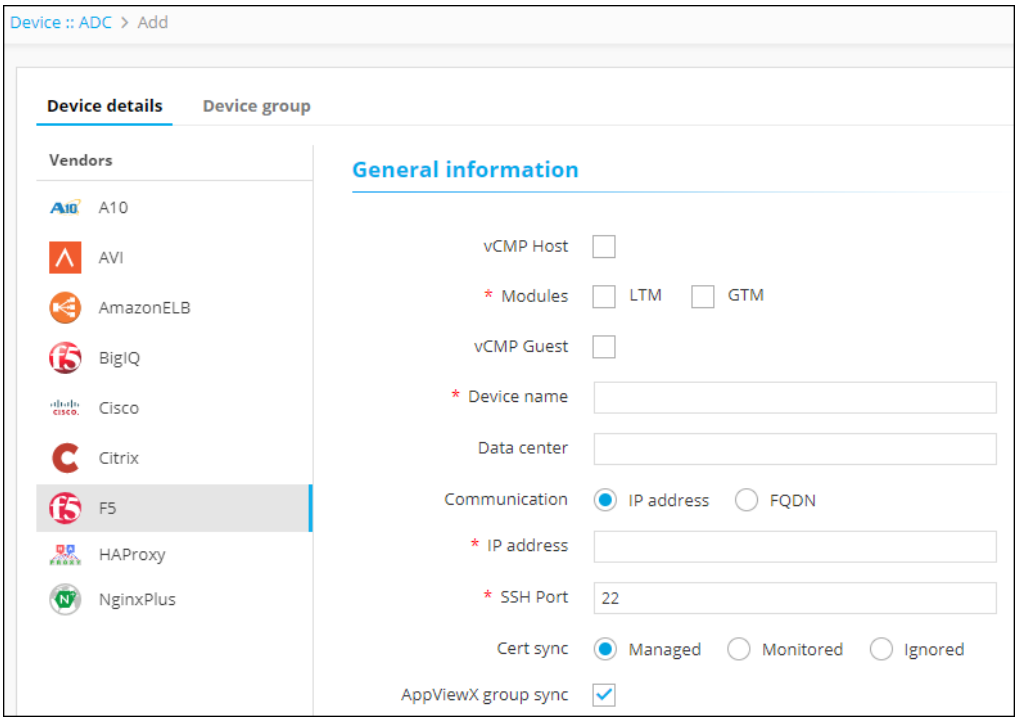
To run this workflow in your environment, the following prerequisites must be met:

- AppViewX version 12.3.0 has been downloaded and installed.
- The device corresponding to the vendor subflow must be added to the AppViewX inventory. The following devices have been added to the AppViewX inventory:
  - F5 LTM or Citrix SLB
  - (Optional) Infloblox or BlueCat
- Each device must be a managed entity in AppViewX.
- The Application user role and Network admin role are created and mapped with respective users.
- In the simple user-form palate settings, the Application owner has been assigned with 'submit' permissions and Network admin has been assigned with 'review' permissions.
- The subflows has been assigned with respective roles.
- (Optional) An ITSM tool, ServiceNow has been configured under the Change Management section of the AppViewX Settings module.

2.1 Add an ADC Device: F5 LTM and Citrix SLB

To add a device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Inventory** > **Device**.
3. The *Device* screen opens with **ADC** device inventory displayed by default.
4. Click the (**Add**) button in the Command bar.
5. On the Add screen that opens, click to select **F5** as the ADC vendor.



6. (Only applicable for F5 device) Click the **vCMP Host** check box, if you want to add and manage the host devices.
7. Select the module (LTM for F5 and SLB for Citrix) to be managed on the ADC device inventory.
8. (Only applicable for F5 device) Click the **vCMP Guest** check box, if you want to add and manage the guest devices.
9. Create a **Device name** that is specific to AppViewX and that will identify the device in the AppViewX inventory.
10. (Only applicable for Citrix device) Enter the **management IP address** of the device.
11. (Only applicable for F5 device) Select the **IP address** or **FQDN** radio button based on how you want to establish the communication.

    Enter the IP address or FQDN in their corresponding fields depending on what you selected.
12. Enter the SSH port number of the device.
13. Specify a **Data center location** if you want to have the option later to filter devices based on their location.

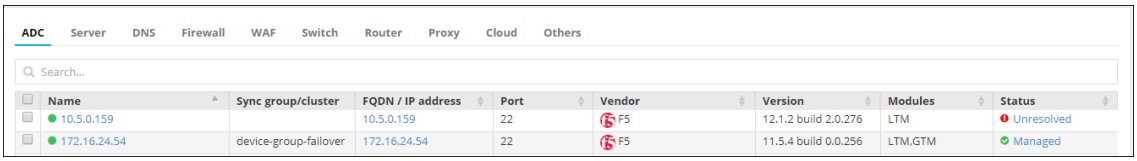
    Note: Ensure that you provide the data center name, else the workflow cannot fetch the data center from where the device are selected.
14. In the **Cert sync** field, select the radio button for the kind of synchronization relationship you want to establish between SSL certificates on the ADC device and AppViewX: **Managed**, **Monitored**, or **Ignored**.
15. (Optional) Select the **AppViewX group sync** check box if you need AppViewX to sync the configuration changes from an active to standby ADC device.

    This is required in older F5 versions like v10. The latest versions of F5 sync automatically.
16. From the **Credential type** dropdown list, select how to want to provide the credentials:
    - Select **Manual entry**, if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.
    - Select **Credential list**, if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the Add a Credential section of this guide.

      When you select the credential name from the dropdown list, the user name and password fields will be auto-filled with the values provided in the credential template.
17. In the **Secondary/Alternate** device field, select how you want to fetch the details of a backup device when the primary device becomes unavailable due to failure or scheduled down time:
    a. Select **Auto detect** if you want AppViewX to automatically detect and retrieve the configuration of the secondary/alternate device, then click Save to add the device to AppViewX.
    b. Select **Manual Entry** if you want to manually provide the details of the secondary device. At a minimum, fill in all fields that contain a red asterisk (*) beside their names.
18. Click **Add** to add the secondary device to the list at the bottom of the screen.

Note: You can add more than one secondary devices. The **Update** and **Delete** buttons are enabled only when you try to modify the existing secondary device.

19. Click **Save** to save the new device in the table on the ADC tab.



The device will display one of the following statuses:

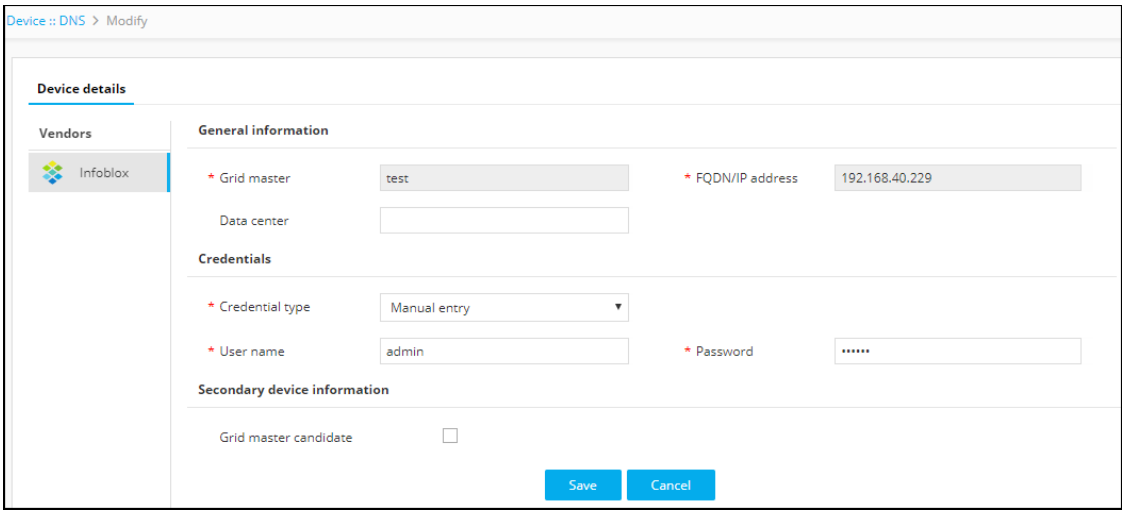
- **In Progress** – Device configuration fetch is in progress.
- **Managed** - Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device due to invalid login credentials.
- **Failed** – Device configuration fetch failed due to unsupported version.

2.2 Add an IPAM Device

2.2.1 Infoblox

To add an Infoblox IPAM device, complete the following steps:

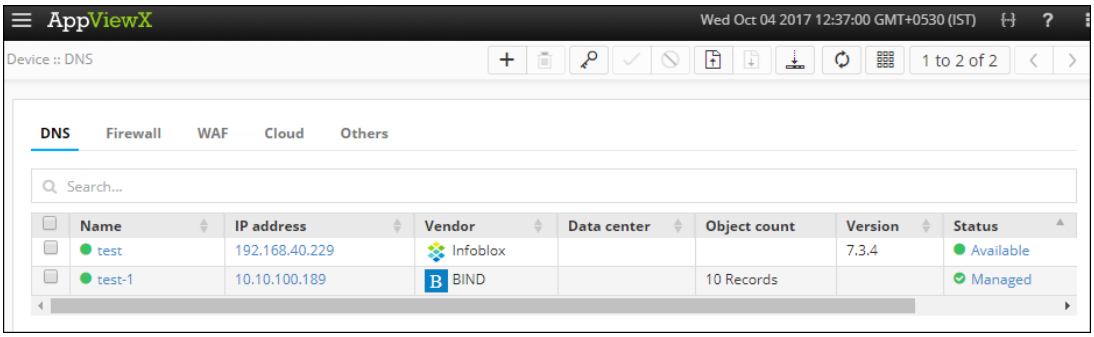
1. Click the (**Menu**) button.
2. Navigate to **Inventory** > **Device**.
   The *Device* screen opens with **ADC** device inventory displayed by default.
3. Click the **DNS** tab.
4. Click the (**Add**) button in the Command bar.
   On the *Add* screen that opens, click to select **Infoblox** as the DNS vendor.



5. In the **Grid master** field, enter a name for the primary device to help users identify it.
6. In the **FQDN/IP address** field, enter the IP address of the primary device for which you want to establish the connection.

7. (Optional) In the **Data center** field, enter the data center name in which the device resides.
8. From the **Credential type** dropdown list, select how to want to provide the credentials:
    - Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the primary device is accessed.
    - Select **Credential list** if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the Add a Credential section of this guide. After you select the credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
9. Click **Grid master candidate** checkbox if you want to add a secondary device.
10. At a minimum, fill in all fields that contain a red asterisk (*) beside their names.
11. Click **Add** to add the secondary device to the table at the bottom of the screen.

    Note: You can add more than one secondary device. The **Update** and **Delete** buttons are enabled only when you try to modify the existing secondary devices.
12. Click **Save** to add the new device in the table on the DNS tab.



The device will display one of the following statuses:

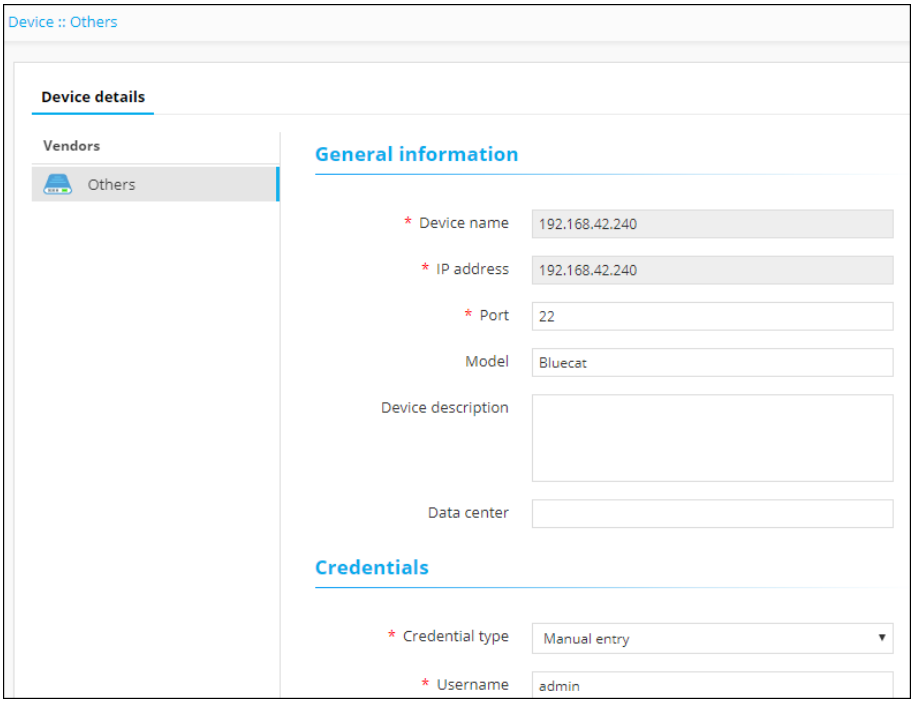
- **In Progress** – Device configuration fetch is in progress.
- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added ADC device should have.
- **Unresolved** – Unable to communicate with device, due to invalid login credentials.
- **Failed** – Device configuration fetch failed, due to unsupported version.

2.2.2 BlueCat

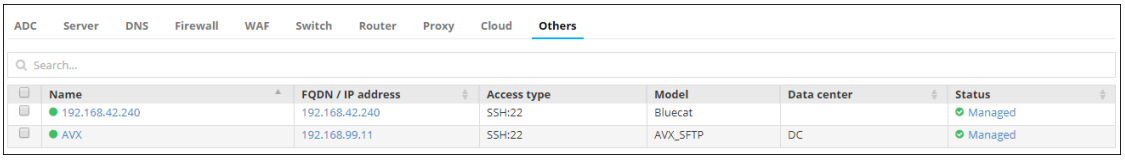
To add the BlueCat IPAM device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Inventory** > **Device**.

   The *Device* screen opens with **ADC** device inventory displayed by default.
3. Click the **Others** tab.
4. Click the (**Add**) button in the Command bar.



5. Enter a name for the device to help the users identify it.
6. In the **IP address** field, enter the IP address of a device for which you want to establish the connection.
7. In the **Port** field, enter a port number through which you want to establish a network connection.
8. (Optional) In the **Model** field, enter the name of the IPAM device vendor (BlueCat).
9. Enter a description of the device that makes it easy for users to tell what the device is for.
10. In the **Data center** field, enter the data center name in which the device resides.
11. From the **Credential type** dropdown list, select how to want to provide the credentials:
    - Select **Manual entry** if you want to manually enter the credential details (user name and the associated password) every time the device is accessed.
    - Select **Credential list** if you want to retrieve the login details created in the credential template. For more details on how to add a credential to a device, refer to the Add a Credential section of this guide. After you select a credential name from the dropdown list, the **user name** and **password** fields are auto-populated with the values provided in the credential template.
12. Click **Save** to add the new device in the table on the **Others** tab.



The device will display one of the following statuses:

- **In Progress** – Device configuration fetch is in progress.

- **Managed** – Device configurations are fetched and parsed successfully. This is the status a successfully added device should have.
- **Unresolved** – Unable to communicate with device due to invalid login credentials.
- **Failed** – Device configuration fetch failed due to unsupported version.

2.3 Create a Role

To create a role, complete the following steps:

1. Click the  (**Menu**) button.
2. Navigate to **Account** > **Role**.
3. Click the  (**Add**) button in the Command bar.
4. On the **Information** tab, specify a role name corresponding to the user (Application owner or Network admin) for whom the role is created for.
5. (Optional) Enter a brief description of what users assigned to the role are able to do and/or what features or functionalities are associated with the role.
6. Click **Save**.
7. In the **Authorized functions** tab, do the following:
    - The role created for the Application owner can only submit the request and provide access to the following functionalities
        - **ADC** > **Control Center** > **Dashboard** > **Inventory**
        - **General** > **Dashboard** > **Create / Delete**
        - **Workflow** > **Request**.
    - The role created for the Network admin can review and approve the request and provide access for all the functionalities.
8. Click the **Access Control** tab and select **Workflow Requests** > **Modular Persona Based Virtual Server Creation**.
9. The ADC component has two additional fields that allow you to assign *global* permissions for orphan and secondary ADC objects to the role you are creating. Users cannot assign *individual* permissions to orphan and secondary objects.
10. To enable this ability, complete the following sub-steps:
    a. Click the **ADC** tab.
    b. Under the **Search** field, select the check box beside **Orphan** if you want to assign global permissions for orphan objects.
    c. Click either the **R** or **RW** icon to give users assigned to the role Read-Only or Read/Write permissions on all orphan objects.
    d. Select the check box beside **Secondary** if you want to assign global permissions for secondary objects.
    e. Click the **R** icon to give users assigned to the role Read-Only permissions on all secondary objects. The RW icon is not available because you cannot grant Read/Write access to secondary objects.
11. Click **Save**.
12. When you have finished assigning components to the role, click the **Provisioning workflow** tab at the top of the screen.

Provisioning workflow allows you to determine which workflows or workflow components you want to associate with the role you are creating.

13. Select the check box beside each workflow you want to associate with the role or click the (**More details**) icon beside a workflow name to view and select the components of the work-flow you want to associate with the role.
14. When you are done, click **Save**.

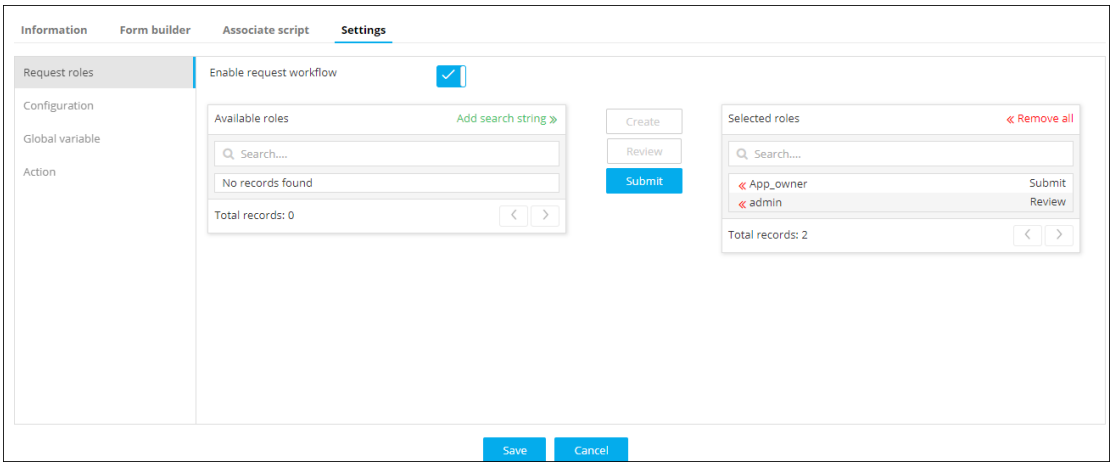
2.4 Assign the Subflows with respective roles

To assign a role to the subflows, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Studio**.
3. Select the *Modular Persona Based Virtual Server Creation*.

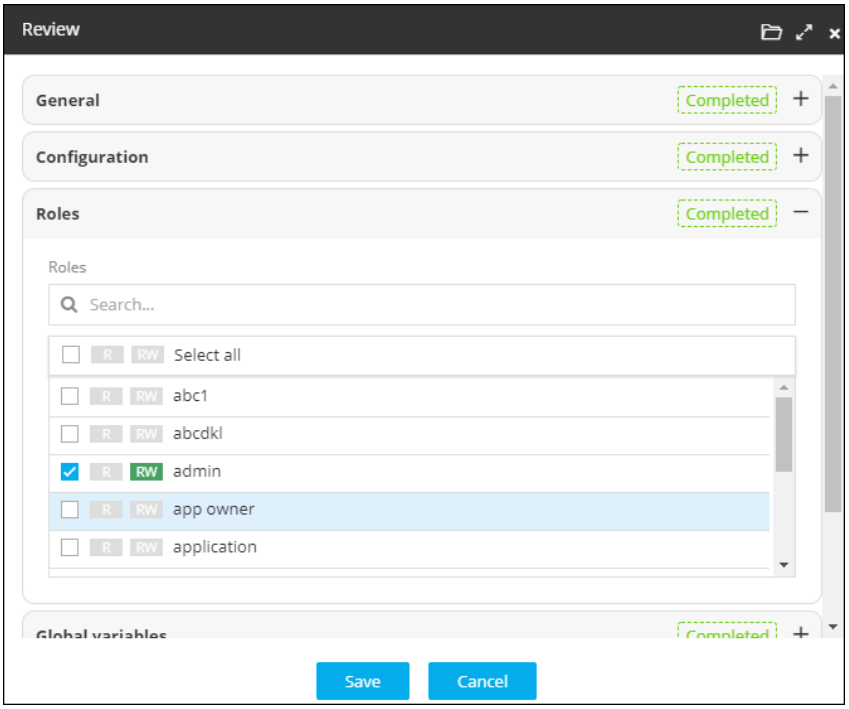
   Note: You can also search for this workflow using the Search box.
4. On the workspace that opens, double-click the subflow (Application Owner User Form, InfoBlox Integration Form, BlueCat Integration Form, Service Now Integration, F5 Virtual Server Creation, or Citrix Virtual Server Creation) to which you want to assign a role.

   The *configuration* screen opens with the **Information** tab selected by default.
5. Click the **Settings** tab.



6. Under the **Request Roles** sub-tab, do the following:
   a. Select the role created for an Application owner from the Available roles and click the Submit button to provide review access.
   b. Select the role created for the Network admin from the Available roles and click the Review button to provide submit access.
   c. Click **Save** to update the changes.

   Note: An application owner will have access only to submit the simple user form and will not have access to the other user forms. The network admin will have access to review the simple user form and submit the other user forms.
7. Open the **Review** or **Approval** subflow from the workspace and click **Roles.**

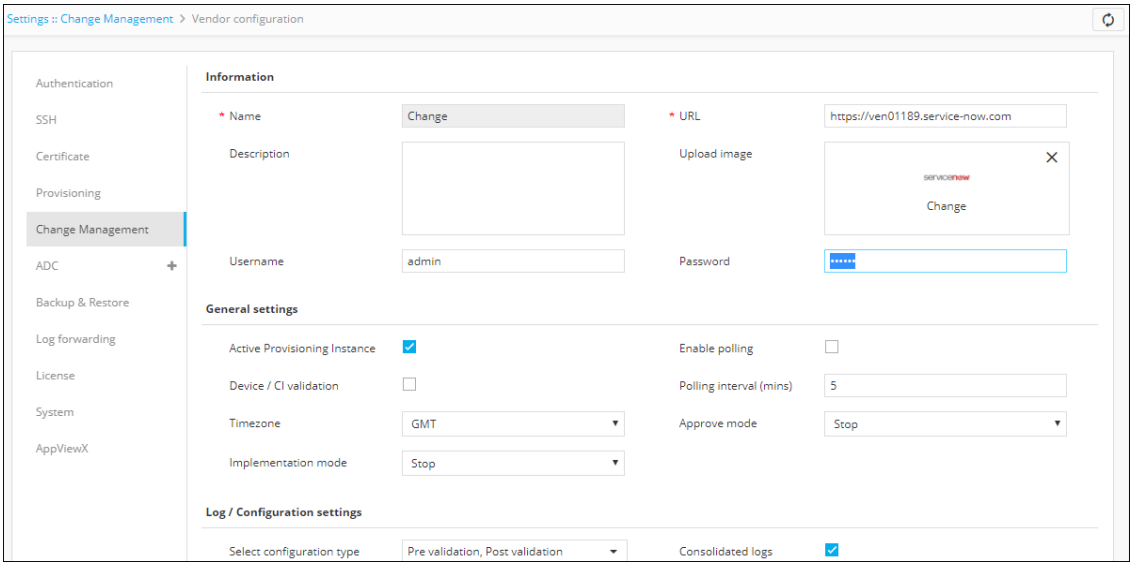


8. Select the role created for an Application owner from the Available roles and click R to provide review access to this role.
9. Select the role created for the Network admin from the Available roles and click RW to provide edit access to this role.
10. Click **Save** to update the changes.

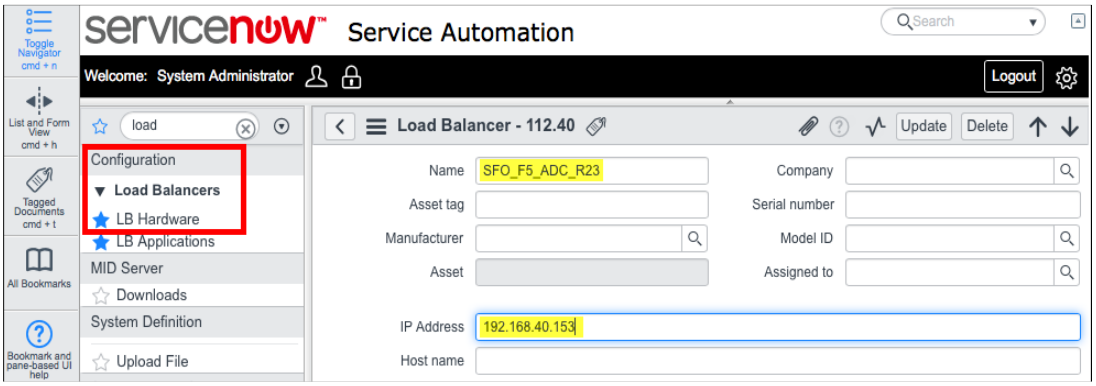
2.5 Register an ITSM Device: ServiceNow

To configure the ITSM device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Settings** > **Change Management**.
3. Click the **ServiceNow** plug-in.
4. On the *Vendor configuration* screen that opens, enter a valid web URL
5. (Optional) Enter a **Description** of the vendor to help users identify it.
6. Enter the ServiceNow **username** and **password** credentials in the respective fields.
7. Click **Update** to save the changes made in the system.



8. (Optional) The F5 LTM or the Citrix SLB device you are configuring should be present in the ServiceNow LB Hardware inventory. You can check this by opening ServiceNow and clicking to open the **Load Balancers > LB Hardware** section shown below. The device name used in the ServiceNow inventory and AppViewX ADC device inventory should be the same.



3 Compatible Software Versions

This workflow has been validated for the following software versions:

- AppViewX – v12.3.0
- F5 (LTM) – v11.x, v12.x, and v13.x
- Citrix – v11.x and v12.x
- Infoblox – v7.2.x
- BlueCat – v8.1.0
- ServiceNow – Geneva, Eureka, Istanbul, and Jakarta

4 Limitations

Auto-trigger option in visual workflow is not working for the first option fetched from the user form.

5 Log In to AppViewX

Log in to the AppViewX web interface. The standard format for a login URL is: `http://hostname`

The default web credentials are set to `admin/AppViewX@123`.

Note: It is recommended that you access AppViewX using Internet Explorer (Version 11.0.9600.18817), Firefox (Version 59.0) or Google Chrome (Version 64.0.3282.186).

6 Preliminary Tasks

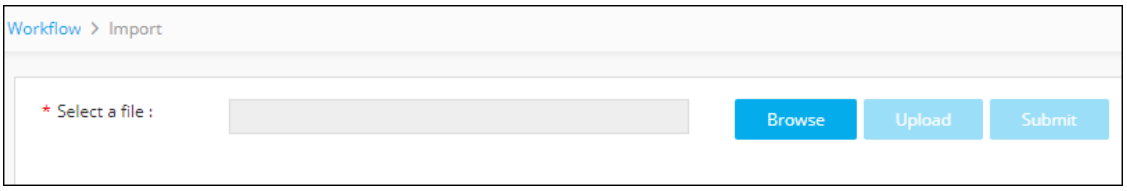
Following are the preliminary tasks that needs to be performed before executing a workflow:

- Import a Workflow
- Import a Helper Script
- Modify the Workflow to Integrate Different Vendors
- Enable a Workflow

6.1 Import a Workflow

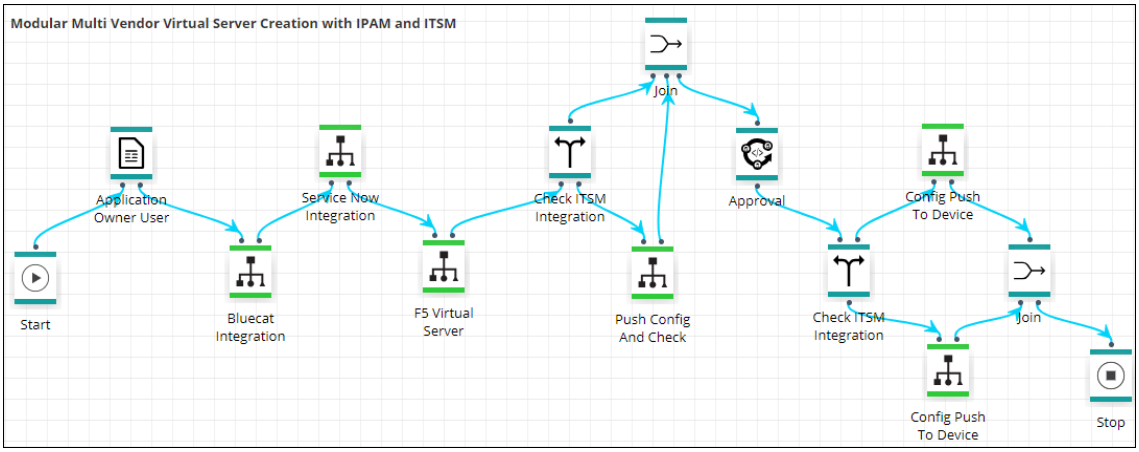
To import the workflow, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click the (**Import**) button in the Command bar.



4. To import a workflow, complete the following sub-steps:
    a. Click the **Browse** button.
    b. Select the zip file containing one or more workflows, then click **Upload**.
    c. In the table at the bottom of the *Import* page, select the check box beside the unzipped workflow file.
    d. Click **Submit** to deploy the workflow into your AppViewX environment.

The Modular Persona Based Virtual Server Creation workflow is shown in the image below:

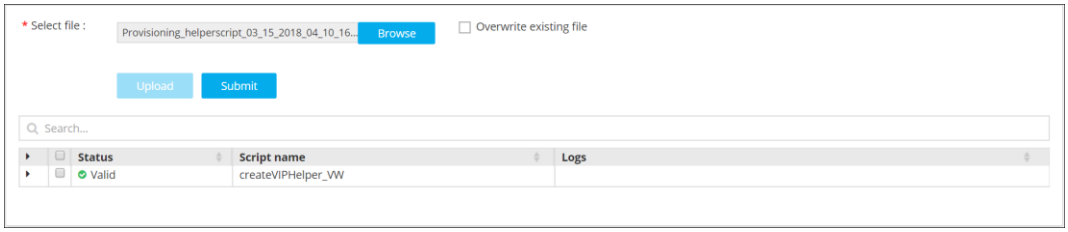


You can modify the vendors of IPAM and ADC devices. For more details on how to modify the vendors, refer to the Modify the Workflow to Integrate Different Vendors section in this guide.

6.2 Import a Helper Script

To import a helper script, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow > Studio**.
3. Click on the (**Helper script**) button. The *Helper script library* screen appears.
4. Click the (**Import**) button.
5. Click **Browse** and select the helper script zip file you want to import.
6. Click **Upload** to import the file and view its contents.



Note: Select the checkbox **Overwrite existing file**, only if the names of the new script file that you are trying to upload and the existing script file are the same.

7. In the table at the bottom of the Import page, select the check boxes beside each of the helper scripts.
8. Click **Submit** to deploy them into your AppViewX environment.

6.3 Modify the Workflow to Integrate Different Vendors

To modify the workflow to support different vendors, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Studio.**
3. Select the *Modular Persona Based Virtual Server Creation* workflow. **Note:** You can also search for this workflow using the Search box.

4. Click the (**Disable**) button in the command bar to modify the workflow.
   On the *Confirmation* screen that pops up, click **Yes**.
5. Right-click the task that you want to remove from the workspace and select **Delete**.
   On the *Confirmation* screen that pops up, click **Yes**.
6. Click the workflow cart on the left-hand side of the workspace.
7. Drag and drop the corresponding task and link them as follows:
   - **F5** and **Citrix Virtual Server Creation** – Between Service Now integration and Check ITSM integration subflows.
   - **Infoblox** and **BlueCat Integration** – Between Application Owner User form and Service Now integration subflows.
8. If you are trying to modify the IPAM component, do the following:
   - Double-click the **Stop** subflow.
   - Select the **cleanup** checkbox from the **Rules list**.
   - From the **Associated workflow** dropdown list, select the **Infoblox DNS Record Deletion (RollBack)** or **BlueCat DNS Record Deletion (RollBack)**, corresponding to what want to integrate with the workflow.
   - Click **Save**.
   - Click on **Rollback** tab in the Command bar.
   - Right-click the IPAM component that are currently integrated with the workflow and select **Delete**.
   - Drag and drop the respective component from the cart and link it between **Check IPAM Integration** and **Join** subflows.

6.4 Enable a Workflow

To enable the workflow, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Configurator**.
   The *Workflow* screen opens.
3. Click the (**Select**) button on the Modular Persona Based Virtual Server Creation workflow to enable it. If the workflow is already selected, a (**Deselect**) button appears.
4. Click the (**Enable**) button in the Command bar.
   Note: You can also enable the required workflow from the Card view by clicking the (**Disable**) button.

On the *Confirmation* screen that appears, click **Yes**.

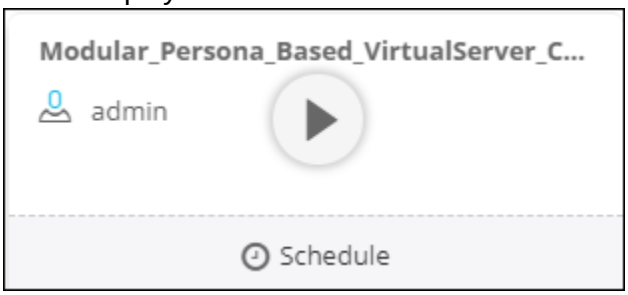
7 Modular Persona Based Virtual Server Creation

To execute the Module Persona Based Virtual Server Creation workflow, complete the following steps:

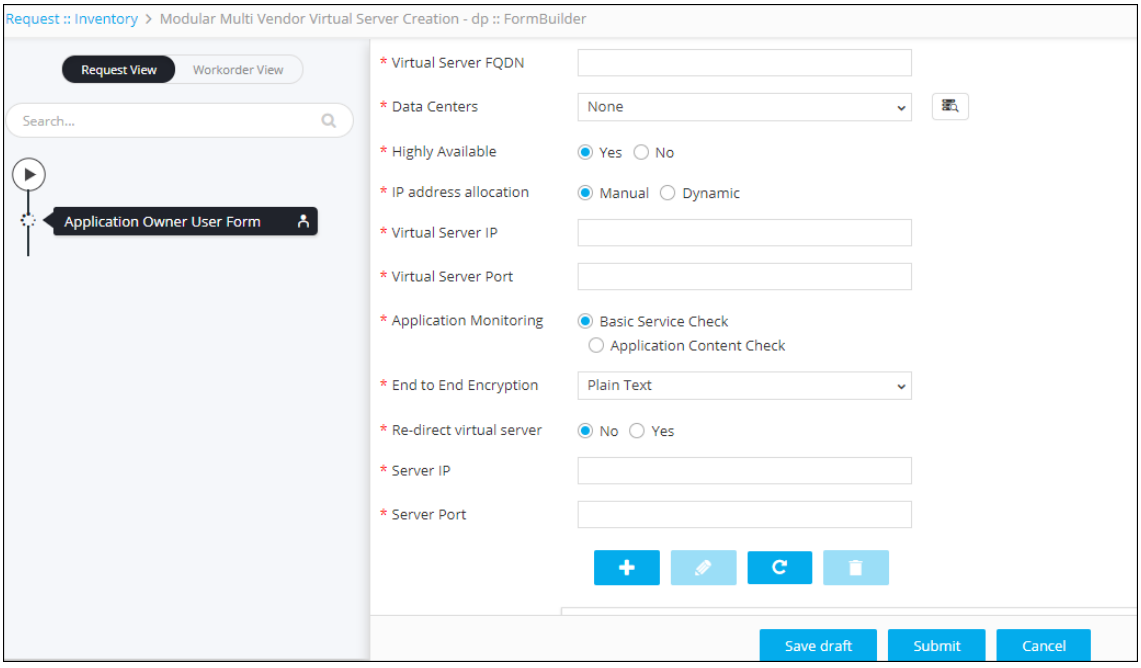
7.1 Application Owner User form

1. Log in to AppViewX using the application owner credentials.
2. Click the  (**Menu**) button.
3. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default. This screen displays all enabled workflows assigned to a specific user role.
4. Click the play button on the *Modular Persona Based Virtual Server Creation* workflow.



5. The **Application Owner User Form** opens with the **Request View** tab displayed by default. Fill in the following form fields:



   a. Enter an FQDN for the application to help the users identify it.

b. In the **Data center** field, click the  (**Retrieve field values**) button to fetch the list of available data centers. Select the data center where the application resides.

   Note: Ensure that you provide the data center name, else the workflow cannot fetch the data center from where the device are selected.

c. Select the **Yes** or **No** radio button based on whether you want the application to be highly available in the data center for user selection. The application will be provisioned on device with a standby if high-availability is selected.

d. Select the **Yes** or **No** radio button if you want to redirect the traffic on http (port 80) to https (port 443).

e. Select the **Manual** or **Dynamic** radio button based on whether you want to integrate the IPAM device to allocate the dynamic IP address.

f. Enter the virtual IP address of the application. The **Virtual Server IP** field appears only when you select *Manual* in Step e.

g. Enter the virtual server port of the application. The **Virtual Server Port** field appears only when you select *No* in Step d.

h. Select the **Basic Service Check** or **Application Content Check** radio button based on how you want to monitor the application.

   The default TCP level will be monitored if you select *Basic Service Check*.

i. Enter the **Send string** and **Receive string** used for monitoring in the respective fields. These fields appear only when you select *Application Content Check* in Step h.

j. From the **End to End Encryption** dropdown list, select one of the following types of encryption based on which profile is associated.
   - **Plain Text** – No encryption is required and go to Step k.
   - **End to End Encryption** – The traffic between the client and server is encrypted using this method. The default certificate and keys are used to encrypt the traffic between the server and load-balancer.
   - **Client Encryption** – The traffic between the client and server is encrypted using this method. Upload the client certificate and key used for encrypting the traffic between the client and load-balancer.

k. Select one of the following type of persistence to direct the traffic to the same server:
   - **None**
   - **Source Address**
   - **Destination Address**
   - **Cookie**

l. Enter the **IP address** and **port number** of the server where the application is hosted. If the application is hosted on multiple servers, ensure all the server details are added.

m. Click the  (**Add**) button.

If the server details are provided correctly, it will be displayed in the **Server** table at the bottom of the screen. You can modify or delete the details by selecting the check box beside the options in the table and then click either the  (**Update**) or  (**Delete**) button.

n. Select the **Yes** or **No** radio button if you want to integrate **ServiceNow** (SNOW) with this workflow to create a service request for tracking and approval purpose.

o. Click **Submit** to trigger the workflow immediately.

A new **Request ID** is created. To view all requests, refer to the **Error! Reference source not found.** section of this guide.

Note: The application owner can only submit the simple self-service user-form. The access to IPAM, ITSM and advanced user-form are restricted to this user. The request is now submitted to the Network admin.

6. Click the  (**Admin**) button in the top right corner.
7. Click the  button to log out as the application owner.

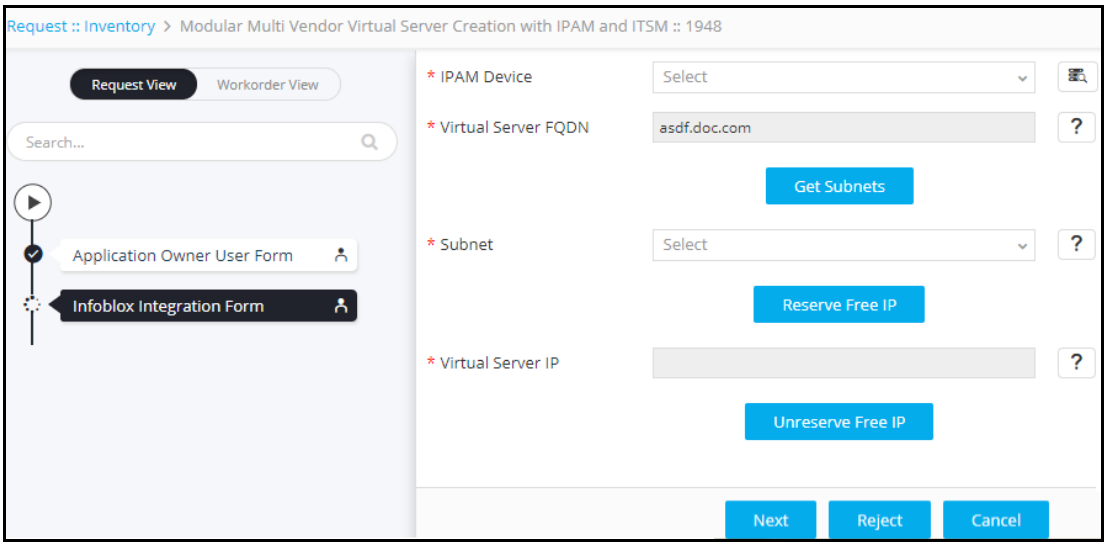
7.2 IPAM Device Integration

The IPAM devices like Infoblox or BlueCat can be integrated to this workflow. This reserves a free IP address from the available address pools and creates DNS binding for the new virtual server.

7.2.1 Infoblox

1. Log in to AppViewX using the Network admin credentials.
2. Navigate to **Workflow** > **Request** > **Request Inventory**.
3. Click the **Request ID** created for Modular Persona Based Virtual Server Creation

   This will display the Application owner user form submitted by the application owner.
4. If *Dynamic* is selected as the **IP address allocation** method in the *Application Owner User Form*, then the corresponding request will be loaded with the IPAM device integration task.
5. If the **Infoblox Integration Form** is linked to this workflow, then the form builder screen will display the following fields:



a. In the **IPAM Device** field, click the (**Retrieve field values**) button to fetch the list of Infoblox devices present in the AppViewX inventory. Select the device you want to integrate with the workflow from the dropdown list.

b. The **Virtual Server FQDN** is a read-only text field that displays the FQDN entered in the *Application User Form*.

c. Click the **Get Subnets** button to retrieve a list of subnets and display them in the **Subnet** dropdown list.

d. Select the subnet to reserve a free IP address.

e. Click the **Reserve Free IP button** to retrieve the free IP address from the selected subnet and display it in the **Virtual Server IP** field.

   A DNS binding (a-record) is created between the virtual server FQDN and the reserved IP address in IPAM system.

f. Click the **Unreserve Free IP** button to delete the DNS binding and release the IP address reserved in Infoblox device.

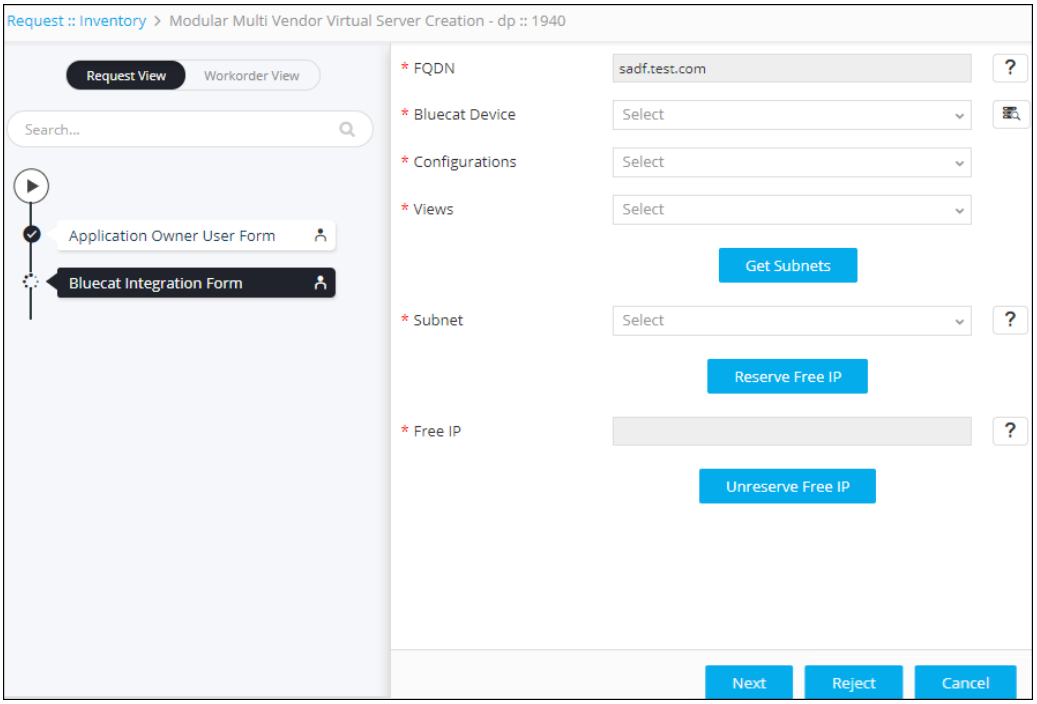
g. Click **Next**.

   On the *Confirmation* screen that appears, click **Ok** to submit the workflow.

7.2.2 BlueCat

1. Log in to AppViewX using the Network admin credentials.
2. Navigate to **Workflow** > **Request** > **Request Inventory**.
3. Click the **Request ID** created for Modular Persona Based Virtual Server Creation.

   This will display the Application owner user form submitted by the application owner.
4. If *Dynamic* is selected as the **IP address allocation** method in the *Application Owner User Form*, then the corresponding request will be loaded with the IPAM device integration task.
5. If the **BlueCat Integration Flow** is linked to this workflow, then the form builder screen will display the following fields:



a. The **FQDN** is a read-only text field that displays the FQDN entered in the *Application User Form*.

b. In the **Bluecat Device** field, click the (**Retrieve field values**) button to fetch the list of BlueCat devices present in the AppViewX inventory. Select the device you want to integrate with the workflow from the dropdown list.

c. Select the configuration of the corresponding BlueCat device. Because, configurations are not retrieved during device addition in the '*Others*' section of AppViewX inventory.

d. Click the **Get Subnets** button to retrieve a list of subnets and display them in the **Subnet** dropdown list.

e. Select the subnet to reserve a free IP address.

f. Click the **Reserve Free IP button** to retrieve the free IP address from the selected subnet and display it in the **Free IP** field

   A DNS binding (a-record) is created between the virtual server FQDN and the reserved IP address in IPAM system.

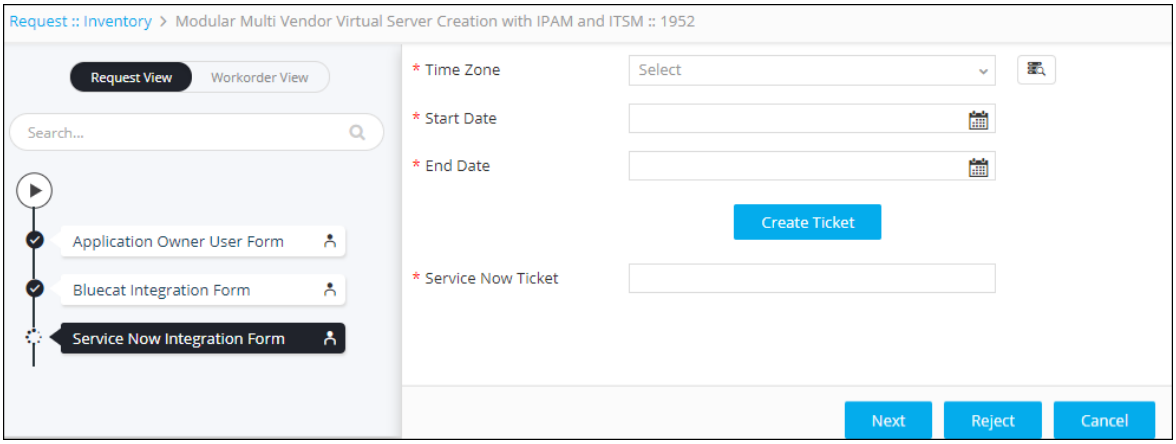
g. Click the **Unreserve Free IP** button to delete the DNS binding and release the IP address reserved in BlueCat device.

h. Click **Next**.

   On the *Confirmation* screen that appears, click Ok to submit the workflow.

7.3 Service Now

If you want to create a service request for tracking and approval purpose using **ServiceNow** (SNOW), the form builder screen is displayed with the following fields:



a. In the **Time Zone** field, click the (**Retrieve field values**) button to fetch all the supported time zones. Select the time zone of the load-balancer device where the configurations will be pushed to.

b. Click the (**Calendar**) button to select the start and end dates and times for the service window. The configuration changes will be implemented during this timeframe

c. Click the **Create Ticket** button to retrieve the ticket number.

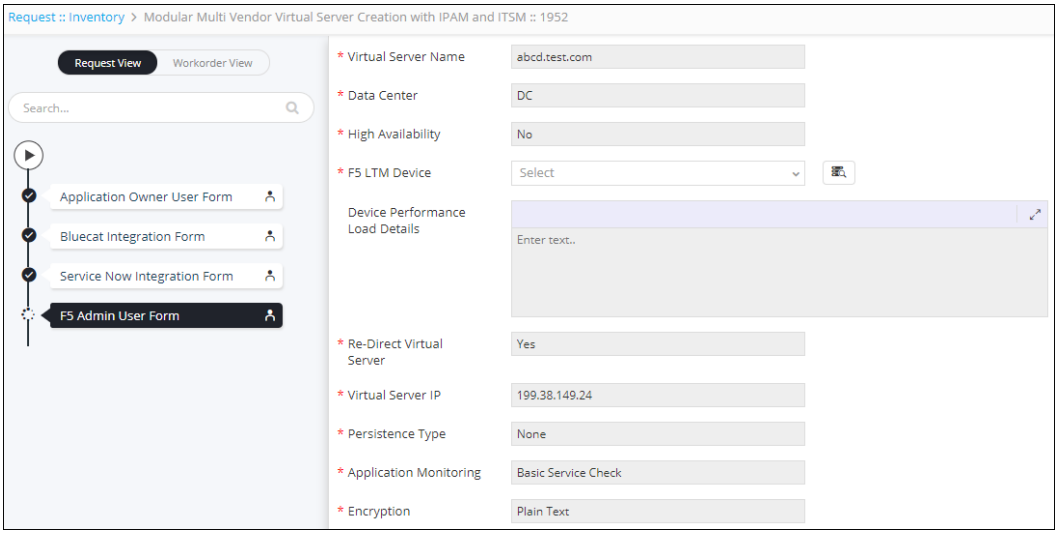
d. The new change request ID will auto populate in the **Service Now Ticket** field.

7.4 Multi-Vendor Device Integration

The workflow enables the user to create a virtual server in the F5 or Citrix devices depending on which vendor has been integrated.

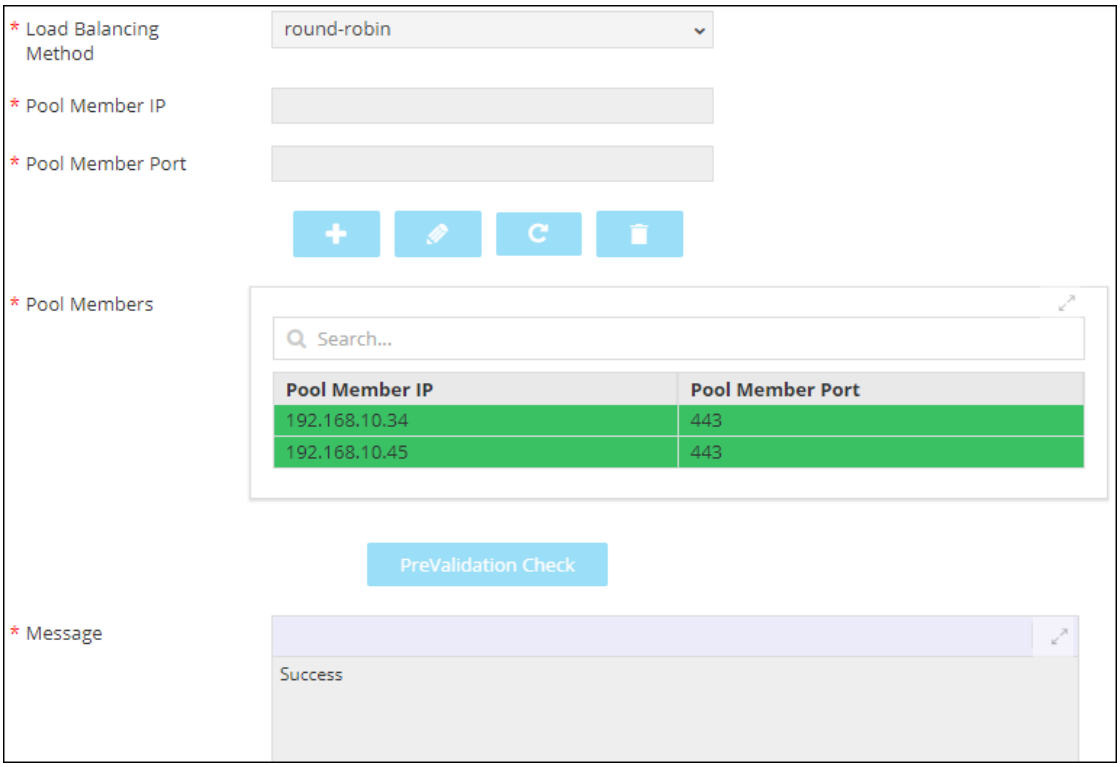
7.4.1 F5 Admin User Form

If the **F5 Admin User Form** is linked to this workflow, the form builder screen is displayed with the following fields:



1. The **Virtual Server FQDN**, **Data Center**, and **High Availability** are the read-only text fields that display what was selected in the *Application User form*.

2. In the **F5 LTM Device** field, click the (**Retrieve field values**) button to fetch the devices based on the data center and high availability selected by the application owner.
3. The **Device Performance Load Details** field provides an information (device memory details) about the selected LTM device. This helps the network admin to check the real-time traffic and performance of the load-balancer device from this user-form, instead of logging into different devices to check these details.
4. The **Re-direct Virtual Server**, **Virtual Server IP**, **Virtual Server Port**, and **Persistence** are the read-only text fields that display what was selected in the *Application User Form*.
5. Based on the type of application monitoring (read-only text field) selected by the application owner, the workflow will automatically create the following monitors:
    - **Application Content Check** – Create and configure a HTTP/HTTPs monitor
    - **Basic Service Check** – Associate the default TCP monitor with the Virtual IP address
6. Based on the encryption type selected by the application owner, the following occurs:
    - **End to End Encryption** – A Client SSL profile with the uploaded certificate and Key is created with the naming convention 'FQDN_clientssl_prof' and the default Server SSL profile will be associated with it.
    - **Client Encryption** – A Client SSL profile with the uploaded certificate and Key is created as FQDN_clientssl_prof
    - **Plain Text** – The SSL profiles are not associated.



7. By default **round-robin** load-balancing method is selected. The admin can update to one of the following load-balancing method from the dropdown list:
    - **ratio-member**

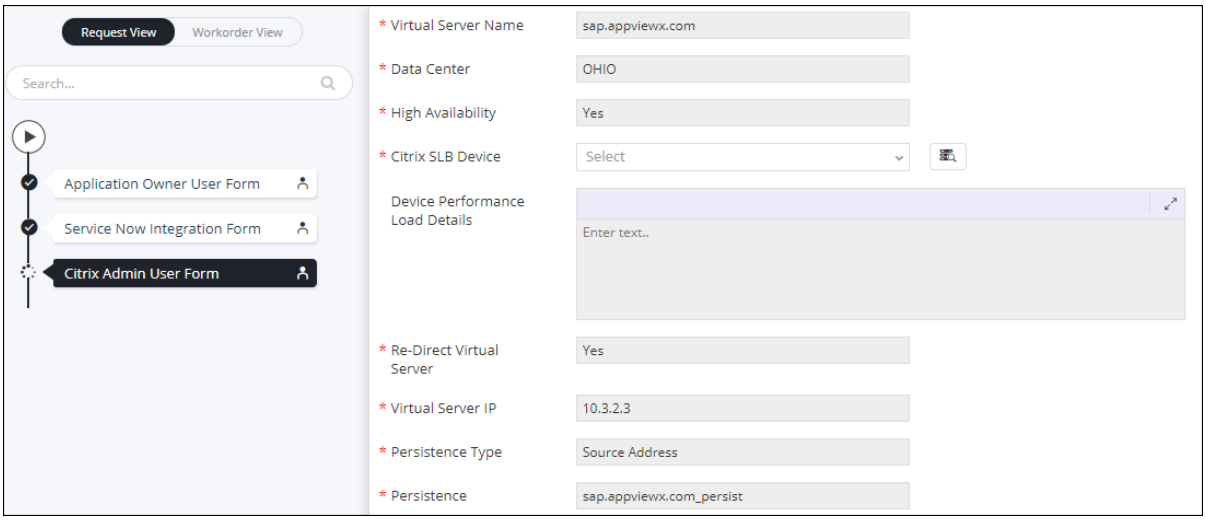
- **least-connections-member**
- **least-connections-node**

8. The **IP address** and **port** number of the pool member are fetched from the Application Owner User form and populated in the **Pool Members** table.

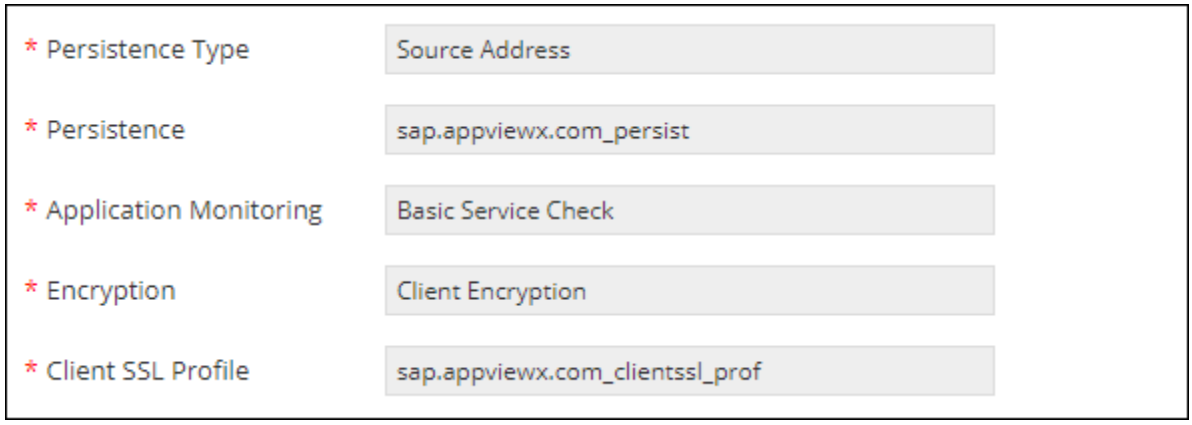
   You can modify or delete the details by selecting the check box beside the options in the table and then click either the  (**Update**) or  (**Delete**) button.
9. Click the **Prevalidation Check** button to ensure if the selected configurations are compatible.
10. In the **Message** field, any error that occurs in the configuration will be displayed.
11. Click **Submit** to trigger the workflow immediately.

7.4.2 Citrix Admin User Form

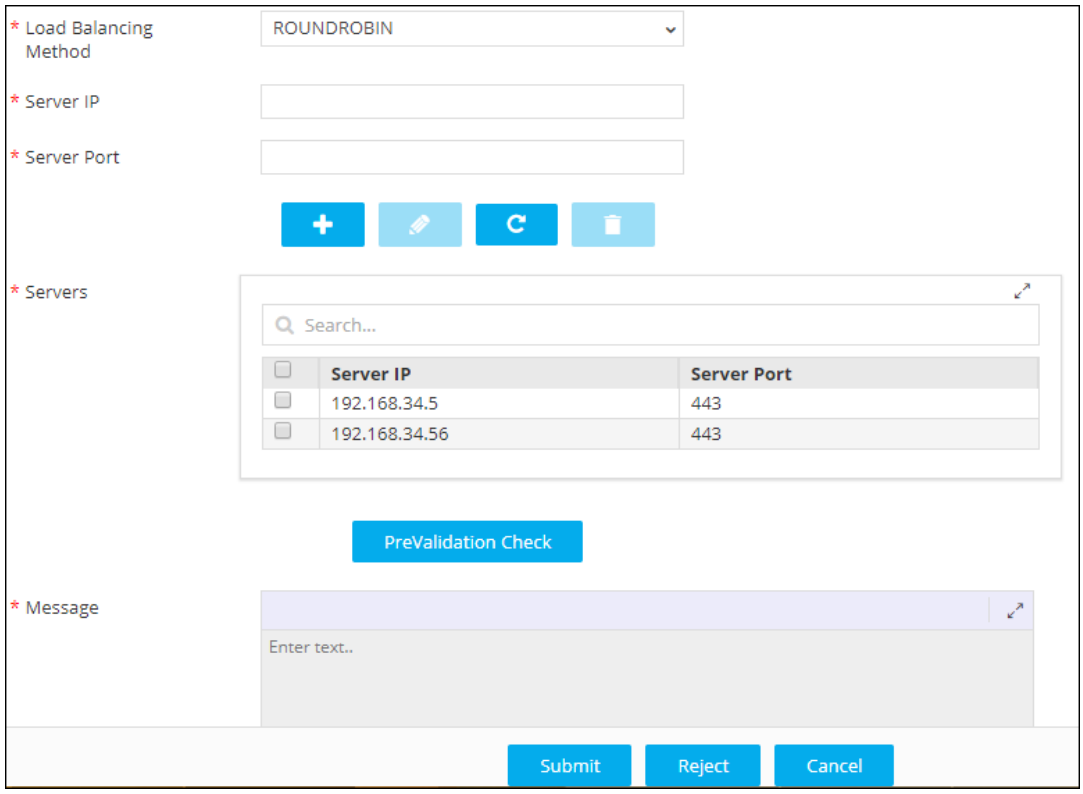
If the **Citrix Admin User Form** is linked to this workflow, the form builder screen is displayed with the following fields:



1. The **Virtual Server FQDN**, **Data Center** and **High Availability** are the read-only text fields that display what was selected in the *Application User form*.
2. In the **Citrix SLB Device** field, click the  (**Retrieve field values**) button to fetch the devices based on the data center and high availability selected by the application owner.
3. The **Device Performance Load Details** field provides an information (device memory details) about the selected SLB device. This helps the network admin to check the real-time load and performance of the load-balancer device from this user-form, instead of logging into different devices to check these details.
4. The **Re-direct Virtual Server**, **Virtual Server IP**, **Virtual Server Port**, **Persistence Type**, and **Persistence** are the read-only text fields that display what you have selected in the *Application User Form*.



5. Based on the type of application monitoring selected by the application owner, the workflow will automatically create the following monitors:
    - **Application Content Check** – Create and configure a HTTP/HTTPs monitor
    - **Basic Service Check** – Associate the default TCP monitor with the Virtual IP address
6. Based on the encryption type selected by the application owner, the following occurs:
    - **End to End Encryption** – A Client SSL profile with the uploaded certificate and Key is created with the naming convention 'FQDN_clientssl_prof' and the default Server SSL profile will be associated with it.
    - **Client Encryption** – A Client SSL profile with the uploaded certificate and Key is created as FQDN_clientssl_prof
    - **Plain Text** – The SSL profiles are not associated.



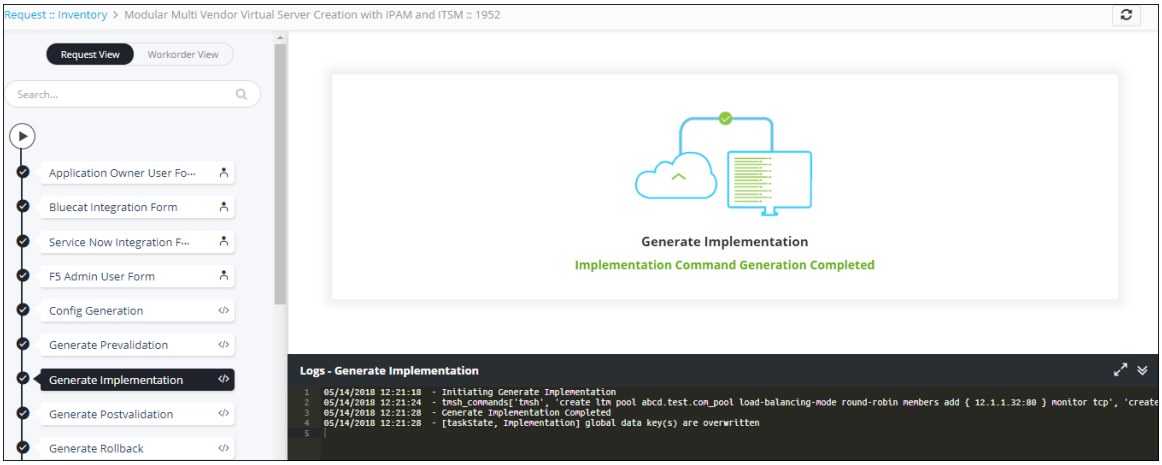
7. By default **round-robin** load-balancing method is selected. The admin role user can update to one of the following load-balancing method from the dropdown list:
    - **ratio-member**
    - **least-connections-member**
    - **least-connections-node**
8. The **IP address** and **port** number of the server are fetched from the Application Owner User form and populated in the **Servers** table.

    You can modify or delete the details by selecting the check box beside the options in the table and then click either the  (**Update**) or  (**Delete**) button.
9. Click the **Prevalidation Check** button to ensure if the selected configurations are compatible.
10. In the **Message** field, any error that occurs in the configuration will be displayed.
11. Click **Submit** to trigger the workflow immediately.

7.5 Workorder Flow

The following are the workorder tasks of Modular Persona based Virtual Server Creation workflow.

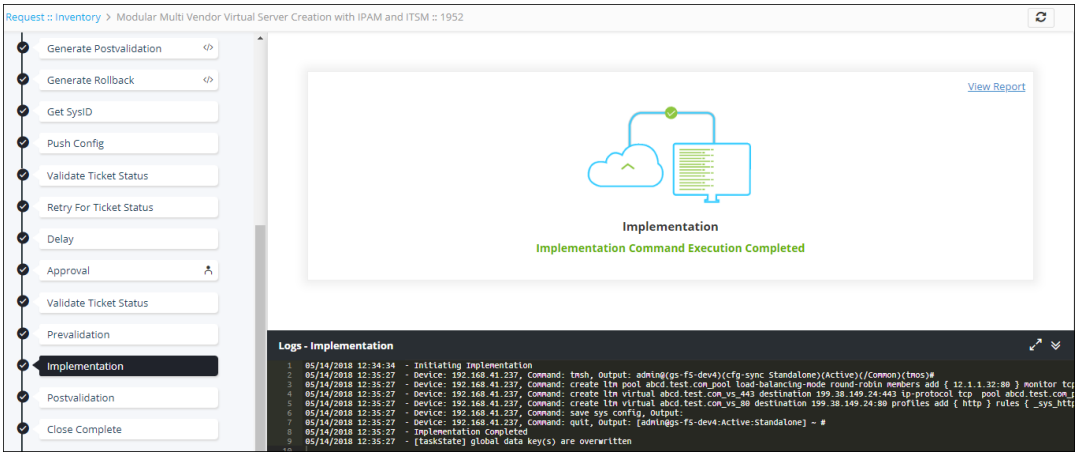
Note: You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.



1. **Application Owner User Form** — A vendor agnostic simple user form that captures the user intent and abstracts the underlying network infrastructure details. Only the Application owner can submit this user form.

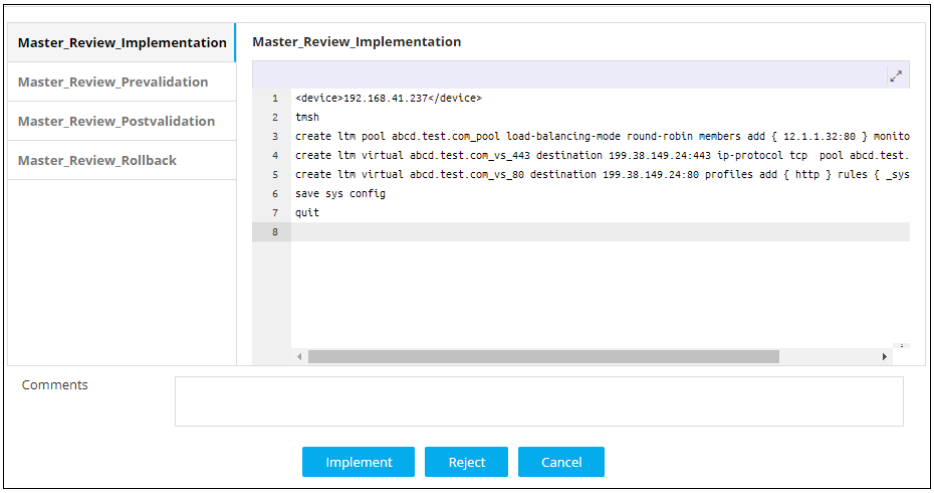
    Note: An application owner cannot access the advanced user-forms whereas the network admin will have access to review the simple user form and submit the advanced user forms.
2. **InfoBlox Integration Form** or **BlueCat Integration Form** — A free IP address is fetched from the device corresponding to what you have integrated and its subnet.
3. **Service Now Integration From** — The change request ID is created based on the inputs provided.

4. **F5 Admin User Form** or **Citrix Admin User Form** — A vendor specific advanced user form that translates the user intent to vendor specific configurations and pre populates most of the values to this form. The Network admin can select the LTM device, add the new application servers, and change the load-balancing method using this form. Also, can view the load on the selected LTM device using this user form.
5. **Config Generation** – This scripted subflow is used to generate the default configuration used for command generation.
6. **Generate Prevalidation** — Prevalidation commands are generated to initiate the prevalidation process.
7. **Generate Implementation** — Configuration commands are generated to create a virtual server in the F5 LTM or Citrix SLB device.
8. **Generate Post Validation** — Postvalidation commands are generated to initiate the postvalidation process.
9. **Generate Rollback** — Configuration commands are generated to delete the virtual server and its LTM objects from a source device. Also, releases the IP address, if it was dynamically allocated from IPAM system.



10. **Generate SysID** — The Sys-ID for the Modular Persona based Virtual Server Creation workflow is generated to track the ServiceNow request.
11. **Push Config** – The configurations that are generated is pushed to the Service Now ticket.
12. **Validate Ticket Status** — Displays the status of ticket validation. To validate the ticket, log in to the ITSM tool-ServiceNow and manually approve the ticket.
13. **Approval** — Approval of a work order is based on the role assigned to the user, who has approval and implementation permissions. After you submit the request form, the configuration changes are reviewed and approved at AppViewX. The Configuration changes are implemented on the device only after approval is received.

    Enter any comments you have related to the implementation, prevalidation, postvalidation, or rollback request and then, click **Implement**.



14. **Validate Ticket Status** – Log in to the ITSM tool-ServiceNow and check the ticket approval status.
15. **Prevalidation** – Check the following
    - A list of virtual servers available in the source device.
    - The virtual server you want to create is not available in the source device.
16. **Implementation** – Configuration commands are implemented, resulting in the creation of a virtual server in the source device.
17. **Postvalidation** – Checks if the virtual server has been created successfully.
18. **Close complete** – After successful creation of the virtual server, the status of the ServiceNow ticket is updated automatically.

8 Rollback a Workorder

A rollback action can be performed only on the completed workflows. To trigger a rollback action, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.
3. The *Request* screen opens with **My catalog** tab displayed by default.
4. Click the **Request Inventory** tab.
5. This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request created for *Modular Persona based Virtual Server Creation* workflow using the **Search** field and/or click the (**Filter**) button.
6. Right-click the request and select **Rollback**.
7. On the Confirmation screen that appears, click **Yes**.
8. Select the **Request** or **Workorder** radio button based on how you want to set the rollback type.
9. Click **Rollback** to trigger the action.

8.1 Workorder Flow

The following are the workorder tasks of *Modular Persona based Virtual Server Creation* workflow.

Note: You can click each task to view its details. Wherever applicable, all logs related to the selected task are displayed in the **Logs** pane at the bottom of the screen.

1. **RollBack Approval1 ─** Rollback of a work order is based on the role assigned to the user, who has approval and implementation permissions. After you submit the request form, the configuration changes are reviewed and approved at AppViewX. The Configuration changes are implemented on the device only after approval is received.
2. **Prevalidation ─** Checks if the virtual server you created is available in the source device.
3. **RollBack ─** The configuration commands are implemented, resulting in the deletion of a newly created virtual server and its LTM objects from a source device.
4. **Postvalidation ─** Checks to see if the virtual server has been deleted successfully.
5. **Infoblox DNS RollBack** – The free IP address reserved in the Infoblox or BlueCat device is released.

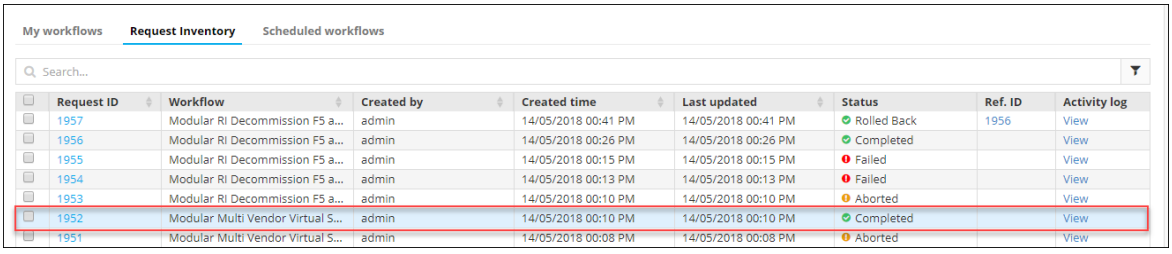
9 Request Inventory

To go to the Request inventory, complete the following steps:

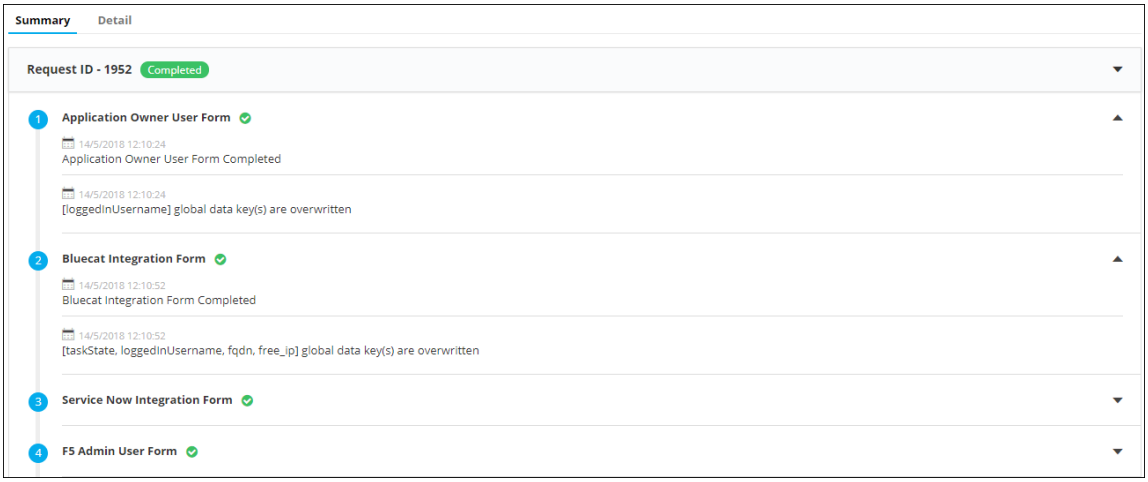
1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the **Request Inventory** tab.

   This displays all workflows that have been triggered. On the **Request Inventory** screen, you can search for a request using the **Search** field and/or click the (**Filter**) button to select the options you want to use to sort the requests.



4. Click the **Request ID** of the requested workflow to view the tasks or phases of a request in a tree-view.
5. You can also view the following details of the request that are created: by whom and when the Request was created, Last updated time, Status and the Activity log.
6. Click **View** in the **Activity log** column to display the request in a stage view. In the **Summary** tab, click the (**Expand**) icon to view the details of each task. Click the **Details** tab to view log messages and other particulars of a request.



10 Schedule a Workflow

To schedule a workflow, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.

   The *Request* screen opens with **My catalog** tab displayed by default.
3. Click the (**Schedule workflow**) button on the respective workflow.
4. On the window that opens, select the frequency of the policy migration process: once, hourly, daily, weekly, monthly, or yearly. The remaining fields in the Scheduler region update depending on the selections you make.
5. Click **Save**.

11 View Scheduled Workflows

To go to the scheduled workflow screen, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Workflow** > **Request**.
3. The *Request* screen opens with **My catalog** tab displayed by default.
4. Click the **Scheduled workflows** tab.
5. On the Scheduled workflow screen that appears, you can perform the following tasks:
   - In the **View log** column, click **View** to display the details of a scheduled workflow.
   - Click the (Pause) or (Resume) button to temporarily stop or continue the execution of a workflow.

12 Add a Credential

To add a credential to a device, complete the following steps:

1. Click the (**Menu**) button.
2. Navigate to **Inventory** > **Device**.

The *Device* screen opens with the **ADC** tab selected by default.

3. Click the respective tab.
4. Click the check box beside the device name, then click the  (**Credential**) button in the Command bar.
5. On the *Add credential* screen that appears, enter the name of the credential you want to add to the device.
6. Enter the **username** and **password** associated with the credential.
7. (Optional) If a secondary credential password was created by a vendor in order to communicate with the device, thus allowing different levels of control over the credential, enter this password in the **Secondary password** field.
8. Click **Save**.

   The credential is then added to the table at the bottom of the screen. You can delete a credential or modify its name, user name, or password by selecting the check box beside the credential name in the table at the bottom of the screen and then clicking either the **Modify credential** or **Delete** button in the Command bar.

13 Troubleshooting

I cannot find the workflow in the Request Catalog

You must enable the workflow from the Configurator section. For more details on how to enable a workflow, refer to the Enable a Workflow section of this guide.

I cannot fetch the ADC device in the user form even after adding it in the AppViewX inventory

Ensure that you provide the data center name while adding a device, else the workflow cannot fetch the data center from where the device are selected.