Configuring the vRealize Automation Plug-in for ServiceNow

Release 2

May 16, 2017

This document supports the version of each product listed and supports all subsequent versions until the document is replaced by a new edition. To check for more recent editions of this document, see http://www.vmware.com/support/pubs.

EN-002402-00

vmware®

You can find the most up-to-date technical documentation on the VMware Web site at:

http://www.vmware.com/support/

The VMware Web site also provides the latest product updates.

If you have comments about this documentation, submit your feedback to:

docfeedback@vmware.com

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

Configuring the vRealize Automation Plug-in for ServiceNow

1

Configuring the vRealize Automation Plug-in for ServiceNow describes installation and configuration information for the vRealize Automation plug-in for ServiceNow. In addition, it provides information about working with the plug-in.

The vRealize Automation plug-in for ServiceNow enables ServiceNow users to deploy virtual machines and perform day 2 actions on CMDB resources using vRealize Automation catalog and governance capabilities.

Intended Audience

This information is intended for ServiceNOW system administrators and other users who install, configure, and use the plug-in.

VMware Technical Publications Glossary

VMware Technical Publications provides a glossary of terms that might be unfamiliar to you. For definitions of terms as they are used in VMware technical documentation, go to http://www.vmware.com/support/pubs.

Preparing for Installation of the vRealize Automation Plug-in for ServiceNow

2

The vRealize Automation plug-in for ServiceNow enables ServiceNow users to deploy virtual machines and perform day 2 actions on CMDB resources using vRealize Automation catalog and governance capabilities.

The vRealize Automation plug-ins for ServiceNow work only with vRealize Automation 7.3, and are available only for the ServiceNow Helsinki and Istanbul releases. Also, the ADFS configuration described herein uses ADFS 2.0. Newer versions of ADFS have not been tested.

The latest version of the plug-in supports both vSphere and Amazon virtual machine provisioning, including day 2 operations like Power ON/OFF, Reboot, and Destroy.

Before configuring ADFS and installing the plug-in, you must configure a Management, Instrumentation, and Discovery (MID) Server to facilitate communication between ServiceNow and vRealize Automation. See http://wiki.servicenow.com/index.php?title=MID_Server_Installation#gsc.tab=0. Note that as part of this installation, you must also set up an appropriate MID Server account.

When you have configured a MID Server, you can proceed to configuring ADFS for both ServiceNow and vRealize Automation.

This chapter includes the following topics:

Configure ADFS Integration with ServiceNow

You can configure Active Directory Federated Services (ADFS) to work with ServiceNow integration. ADFS provides single sign-on access to systems that work in tandem.

Prerequisites

- Download an instance of the ADFS federation metadata file by entering the file URL in your browser: `https://ADFS hostname/federationmetadata/2007-06/federationmetadata.xml`

  One instance of this file supports vRealize Automation integration with ADFS, and another supports ServiceNow integration with ADFS.

Procedure

1. Log in to ServiceNow as an administrator.
2. Select **Plugins** and then search for SSO plug-in by entering SSO in the Plug-in search.
3. Verify that the plug-in titled "SSO provided by Okta, Inc." is activated.

4 Configure properties for the ServiceNow identity provider.

   a As a ServiceNow system administrator, enter SAML in your Filter to navigate to the SAML Single SignOn.

   b Select **Properties** to configure SAML sign on properties.

   c Select the **Enable external authentication** check box.

5 Open the ServiceNow federation metadata file that you downloaded, and use the appropriate information from the file to populate text boxes on the SAML 2.0 Single Sign-on properties page.

ServiceNow SAML Single Sign-on Setting	Example Value
The Identity Provider URL which will issue the SAML2 security token with user info.	http://*ADFS host name*/adfs/services/trust
The base URL to the Identity Provider's AuthRequest service. The AuthRequest will be posted to this URL as the SAMLRequest parameter.	https://*ADFS host name*/adfs/ls/
The base URL to the Identity Provider's SingleLogoutRequest service. The LogoutRequest will be posted to this URL as the SAMLRequest parameter.	https://*ADFS host name*/adfs/ls/?wa=wsignout1.0
The protocol binding for the Identity Provider's SingleLogoutRequest (Values can be either "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect" or "urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST".)	urn:oasis:names:tc:SAML:2.0:bindings:HTTP-Redirect For most systems, you can accept the default.
SignLogoutRequest. Set this property to true if the Identity Provider's SingleLogoutRequest service requires signed LogoutRequest.	Optional or leave blank.
URL to redirect users after logout, typically back to the portal that enabled the SSO (e.g. http://portal.companya.com/logout)	external_logout_complete.do

6 Configure ServiceNow Service Provider properties.

   Keep defaults for all fields not listed in the following table.

Property	Example
The URL for the ServiceNow instance home page.	https://*ServiceNow instance name*/navpage.do
The entity identification or the issuer	https://*ServiceNow instance name*
The audience uri that accepts SAML2 token.	https://*ServiceNow instance name*
The User table field to match the Subject's NameID in the SAMLResponse.	email
The NameID policy to use for returning the Subject's NameID in the SAMLResponse. The SAML identity provider must support this by declaring the policy in its metadata. The NameID value is used to match with the specified field in the User table to lookup the user.	urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress

7 Click **Save**.

What to do next

Configure the SAML 2.0 certificate for ServiceNow.

1 Open your ServiceNow certificate in a text editor.

2 Click the certificate link in the SAML plug-in section of the certificate.

3 Navigate to the IDPSSODescriptor KeyDescriptor signing x509Data section of the Federation.xml file.

4 Copy the certificate content from <X509Certificate> node in federation metadata.xml file.

```
<KeyDescriptor use="signing">  <KeyInfo xmlns="http://www.w3.org/2000/09/xmldsig#">
<X509Data>
<X509Certificate>
MIIC4jCCAcqgAwIBAgIQR
+DHGU933YhJuHDY6OIXYDANBgkqhkiG9w0BAQsFADAtMSswKQYDVQQDEyJBREZTIFNpZ25pbmcgLSBhZGZzLTAxYS5jb3
JwLmxvY2FsMB4XDTE2MDQxNTEzNDMxMFoXDTE3MDQxNTEzNDMxMFowLTErMCkGA1UEAxMiQURGUyBTaWduaW5nIC0gYWR
mcy0wMWEuY29ycC5sb2NhbDCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAOrs7dBB2hjpqwuLpQzxQ
+bHisF5bOjFcuAkjOsD1fBCvOGYv8dNhPgRY4CniLB5ZiH3KJEvxGr3meP00qFRuyG/1gsdHP2+0IBw9AUxb9D22ypEgo
mAN0ygOm2aCtggQUY9GlOu5qUEKTvOC/284p
+WK/MweE/A93ujk28qnYPjfEvhiFA8IcxMXh6souptcI28+xHYtE5O5TrEdlck3uSzmfpsQlmaVBPiqlhLIuM5VfdhOC9
oFkMnesvisvDPrTUahSx3Jq7wtO808rtCytw6gDdVzwmYKBR/Kq3BZ24JuWisBnhKeVGvZp538gErjspc2FzKO41xz9mE
zPTCfRECAwEAATANBgkqhkiG9w0BAQsFAAOCAQEAkilkY1SkKmCYOrZ/y3NjYY3bcyhsgknleFKVNfsQ5DLytS
+kd2uQpWiqI/kywcuW0ZBj+xm28R/uqGBx27e+/jLJAQiOGOwT6XJU09z3AmCg9AZ
+qD8EXuucH9iPjYzacHNHYDLFEiy7d31H8Mg+EajjWO
+OC00vBPeOno2lUoJLOK6SoIlgIDgRZcYK9r7DSp8hhDDg8GervYpHnAr9AsW8zz1puuoy
+oVVeIb7OlxcUnZpydAsGEPDSwzcW1iAMnhBgxcm7HwLUt2MS4IZUpaAXC8m/BpJt1xcbhy/IaqLyC8yEw6fBSK5hddTc
YacnFGQSUhguh/ZoyJaIcuocA==
</X509Certificate>
</X509Data> </KeyInfo> </KeyDescriptor>
```

5 Paste this certificate content in between -----BEGIN CERTIFICATE----- and -----END CERTIFICATE----- PEM Certificate Text Box.

6 Right click on the toolbar and select **Save**.

7 Click the Validate link at the bottom of page to validate your certificate.

8 Verify the fields Valid from, Expires, Short description, Issuer and Subject are parsed correctly from the certificate.

9 Click **Update**.

10 Click the Metadata link in the SAML plug-in menu and copy the metadata content to an xml file: for instance, `servicenowInstanceName–metadata.xml`.

Configure an ADFS Relying Party Trust with ServiceNow

You can set up an ADFS relying party trust in ServiceNow. A relying party trust object uses a identifiers names and rules to identify a web application to the Federation Service.

Procedure

1 Log in to your ADFS server by opening Administrative Tools and finding the ADFS console link.

2 Open the ADFS 2.0 Management console and select **Trust Relationships > Relying Party Trusts**.

3 Right-click on **Relying Party Trust** and select **Add Relying Party Trust...**

4 Click **Start** on the configuration wizard.

5 Select **Import data about the relying party from a file** on the Select Data Source page.

6 Import the ServiceNow metadata file that you copied and saved previously from the SAML configuration metadata section.

7 Click **Next**.

8 Enter the name for your ServiceNow instance in the **Display** text box on the Specify Display Name page.

9 Click **Next**.

10 Select **Permit all users to access this relying party** on the Choose Issuance Authorization Rules page.

11 Click **Next**.

12 Click **Next** on the Ready to Add Trust page.

13 Click **Close** on the Finish page.

If the check box for rules was enabled, also click **Cancel** on the Edit Rules page.

Configure Claim Rules for ADFS ServiceNow Integration

When configuring ADFS integration for ServiceNow, you must set up the appropriate claim rules to control the behavior of incoming and outgoing claims.

Prerequisites

Set up the appropriate relying party trust relationship between ServiceNow and ADFS.

Procedure

1 Right click the relying party trust that you created for ServiceNow, and select **Edit Claims Rules**.

2 Select **Add Rule** on the Issuance Transform Rules tab.

3 Select **Send LDAP Attributes as Claims** as the template for the claim rule to create.

4 Click **Next**.

5 Enter the name **`Get Email Attribute`** in the **Claim rule name** text box on the Configure Claim Rule wizard page.

6 Select Active Directory as the **Attribute store**.

7 Select the email addresses for LDAP attributes and the Outgoing Claim Type using the **E-Mail Addresses** drop-down in the Mapping of LDAP attributes to outgoing claim types section of the page.

8 Click **OK**.

9 Click **Finish**.

10 Select **Add Rule**.

You must add a rule that transforms the attributes received from LDAP in the Get Email Attribute rule into the desired SAML format.

11 Select **Transform an Incoming Claim**.

12 Click **Next**.

13 Enter the name **`Transformation`** in the **Claim rule name** text box on the Configure Claim Rule wizard page.

14 Select **E-Mail Address** for the incoming claim type.

15 Select **Name ID** as the outgoing claim type.

16 Select **Email** as the outgoing name ID format.

17 Select **Pass through all claim values**.

18 Click **Finish**.

19 Click **Apply**.

20 Click **OK**.

What to do next

You can now test your ServiceNow ADFS integration. Note that users must have the same email address in both ServiceNow and in the Active Directory connection used by ADFS.

1 Add a domain in ServiceNow that can authenticate to you ADFS.

2 Log in to ServiceNow as a System Admin and select **Users**.

3 Enter an ADFS user complete with email address and password.

4 Select **Update**.

5 Log out of your ServiceNow instance and then log back in as the user that you just created and verify that you are redirected to the ADFS login page.

Configure ADFS Integration with vRealize Automation

As part of SAML configuration to support ADFS integration with vRealize Automation and ServiceNow, you must configure ADFS integration with vRealize Automation.

See *Configuring vRealize Automation* for more information on configuring an Active Directory connection and an Identity Provider in vRealize Automation.

The ITSM plugin currently supports only one tenant per plug-in installation.

Complete the following steps in the tenant that will used and configured with the plug-in.

Prerequisites

- Configure an Active Directory over LDAP connection in vRealize Automation. See the Directories Management documentation in the *Configuring vRealize Automation* publication for more information.
- Download an instance of the ADFS federation metadata file by entering the file URL in your browser: `https://ADFS hostname/federationmetadata/2007-06/federationmetadata.xml`

  One instance of this file supports vRealize Automation integration with ADFS, and another supports ServiceNow integration with ADFS.

Procedure

1 Open the Federation Metadata file that you downloaded for use as part of your vRealize Automation configuration in a text editor.

2 Create a test network range to validate login after vRealize Automation ADFS is configured.

  This network range enables you to correct any configuration issues from a separate machine in case there are any issues that prevent federation from functioning. When you determine that your ADFS is functioning on the test network range, you can enable it to a wider group.

  a Log in as a tenant administrator.

  b Select **Administration > Directories Management > Network Ranges**

  c Select **Add Network Range**.

  d Enter the appropriate values for the network range on the dialog.

Property	Value
Name	My Machine
From	Enter the appropriate IP address.
To	Enter the appropriate IP address.

  e Click **Save**.

3 Create an Identity Provider.

   a Log in as a tenant administrator.

   b Select **Administration > Directories Management > Identity Providers**

   c Select **Add Identity Provider** and then **Create Third Party IDP**.

   d Enter the appropriate values for the network range on the New IdP page.

Property	Value
Identity Provider Name	ADFS Hostname
SAML Metadata	Paste the contents of the FederationMetadata.xml file that you edited and click **Process IdP Metadata**
Users	Check the specified domain
Network	Check My Machine
Authentication Methods	Enter SAML for the authentication method
SAML Context	Select urn:oasis:names:tc:SAML: 2.0:ac:classes:Password from the Authentication Methods drop down menu.
Property NameID Policy Value	Select the emailAddress policy

   e Click Service Provider (SP) Metadata to download the SAML metadata file and save it as `sp.xml`.

   f Click **Add**.

4 Click **Save**.

What to do next

After completing this procedure, configure the default access policy by adding your test network to the top of the stack of network ranges in your default policy. After you configure the policy, you cannot log in from the IP specified in the test network range to the specified domain. If you wish to log in as an domain user, then you must log in from a different machine with a different IP address. See the Add or Edit a Network Range topic in *Configuring vRealize Automation* for more information.

Configure an ADFS Relying Trust with vRealize Automation

You can set up an ADFS relying party trust with vRealize Automation. A relying party trust object uses identifiers, names, and rules to identify a web application to the Federation Service.

You must set up an ADFS relying party trust and the appropriate claims rules.

Procedure

1 Log in to your ADFS server.

2 Open the ADFS 2.0 Management console and select **Trust Relationships > Relying Party Trusts**.

3 Right-click on **Relying Party Trust** and select **Add Relying Party Trust...**.

4 Click **Start** on the configuration wizard.

5 Select **Import data about the relying party from a file** on the Select Data Source page.

6 Import the vRealize Automation Service Provider metadata file, sp.xml, that you copied and saved previously when setting up the Identity Provider.

7 Enter a name for your vRealize Automation appliance instance in the **Display** text box on the Specify Display Name page.

   You can also enter a description for the trust in the **Notes** text box.

8 Click **Next** on the Ready to Add Trust page.

9 Select **Permit all users to access this relying party** on the Choose Issuance Authorization Rules page.

10 Click **Next**.

11 Click **Next** on the Ready to Add Trust page.

12 Click **Close** on the Finish page.

Configure Claim Rules for vRealize Automation ADFS Integration

When configuring ADFS integration for vRealize Automation, you must set up the appropriate claim rules.

Prerequisites

Set up the appropriate relying party trust relationship between vRealize Automation and ADFS.

Procedure

1 Right click the relying party trusts that you created previously, and select **Edit Claims Rules**.

2 Select **Add Rule** on the Issuance Transform Rules tab.

3 Select **Send LDAP Attributes as Claims** as the template for the claim rule to create.

4 Click **Next**.

5 Enter **`Get Attributes`** in the **Claim rule name** text box on the Configure Claim Rule wizard page.

6 Select Active Directory as the **Attribute store**.

7 Select the e-mail addresses for LDAP attributes and Outgoing Claim Type using the **E-Mail Addresses** drop down menu in the Mapping of LDAP attributes to outgoing claim types section of the page.

8 Click **OK**.

9 Click **Finish**.

10 Select **Add Rule**.

You must add a rule that transforms the attributes received from LDAP in the Get Attributes rule into an appropriate SAML format.

11 Select **Send Claims Using a Custom Rule** as the template.

12 Click **Next**.

13 Enter **Transformation** as the claim rule name.

14 Paste the following text into the rule.

```
c:[Type == "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/emailaddress"]
=> issue(Type = "http://schemas.xmlsoap.org/ws/2005/05/identity/claims/nameidentifier",
Issuer = c.Issuer, OriginalIssuer = c.OriginalIssuer, Value = c.Value, ValueType =
c.ValueType,
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/format"] =
"urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress",
Properties["http://schemas.xmlsoap.org/ws/2005/05/identity/claimproperties/spnamequalifier"]
= "vmwareidentity.domain.com");
```

15 Change `vmwareidentity.domain.com` in the last line of the pasted text to your vRealize Automation appliance fully qualified domain name.

16 Click **Apply**.

17 Click **OK**.

Install vRealize Automation Plug-in for ServiceNow

3

The vRealize Automation plug-in for ServiceNow enables ServiceNow users to deploy virtual machines and perform day 2 actions on resources using vRealize Automation catalog and governance capabilities.

When installed, the vRealize Automation plug-in does the following:

- Creates vRealize Automation Catalog and vRealize Automation Resources menu items within the ServiceNow Self-Service module.
- Creates a workflow for requesting vRealize Automation catalog items.
- Creates the catalog admin role and assigns it to the System Administrator.
- Grants the users with the catalog admin role access to the **Integration > vRealize Automation** module.

Prerequisites

- Configure a Management, Instrumentation, and Discovery (MID) Server to facilitate communication between ServiceNow and vRealize Automation. See http://wiki.servicenow.com/index.php?title=MID_Server_Installation#gsc.tab=0. Note that as part of this installation, you must also set up an appropriate MID Server account.

  If you are creating a MID Server in the ServiceNow Helsinki release, you must validate you MID Server before installing the plug-in.

  a Log in as a System Administrator.

  b Enter MID in the search box to locate the MID Server configuration section.

  c Click Servers and verify that your installed MID Server has a Status of UP and the Validated column shows `No`.

  d Click the box next to your MID Server name.

  e Select **Validate** in Actions on selected rows.

  f Verify that Yes is displayed for Validated on the Dashboard.
- Configure an Active Directory link for vRealize Automation. See *Configuring vRealize Automation* for more information.
- Configure Active Directory Federated Services for vRealize Automation and for ServiceNow. See "Configure ADFS Integration with vRealize Automation," on page 11 and "Configure ADFS Integration with ServiceNow," on page 7.
- Download the appropriate version of thevRealize Automation ServiceNow plug-in from the Solution Exchange for your ServiceNow version, either Helsinki or Istanbul.

Procedure

1 Log in to the ServiceNow portal as a system administrator.

2 Select **System Update Sets > Retrieved Update Sets**.

3 Place the cursor on the **Retrieve Update Sets** queue and then select **Import Update Set from XML** from the displayed menu.

4 Click **Browse** on the dialog to choose the file to upload, and then select the vRealize Automation ServiceNow XML file.

5 Click **Upload**.

6 In the Retrieved Update Sets list, select the vRealize Automation ServiceNow update set in the Name column and then **Loaded** in the State column.

7 Select **Preview Update Set** to validate the update set before committing it.

A dialog box confirms update set validation.

8 Inspect the update set information, and then click **Commit Update Set**.

A dialog box opens automatically after you click **Commit Update Set** while the commit action is in progress. A **Close** button appears on the dialog when the commit completes. Click this button to dismiss the dialog.

9 Click **Update Set logs** .

The install is complete when a message appears stating `Finished update load from database`.

10 Select **Retrieved Update Sets** in the left menu and verify that the VMware update set has a status of Committed.

What to do next

After the plug-in is installed, you must configure it to function within ServiceNow.

This chapter includes the following topics:

Set up Users for the vRealize Automation Plug-in for ServiceNow

You can configure users either before or after installing the vRealize Automation plug-in for ServiceNow.

If ADFS is configured for single sign on as described herein, it relies on the email address of users to be the same in vRealize Automation and ServiceNow. As a best practice, set up your users in both systems with the same email address.

See Chapter 4, "Using the vRealize Automation Plug-in for ServiceNow," on page 29 for information about logging in.

Note The ADFS configuration described herein impacts all users in vRealize Automation and ServiceNow. ADFS allows log in for vRealize Automation users that are not in ServiceNow. It does not allow log in for ServiceNow users that are not in vRealize Automation.

Prerequisites

Install the vRealize Automation plug-in for ServiceNow. See Chapter 3, "Install vRealize Automation Plug-in for ServiceNow," on page 15.

Procedure

- Verify and, if necessary, update the appropriate users and roles in ServiceNow. See http://wiki.servicenow.com/index.php?title=Creating_Users_and_Associating_to_a_Group#gsc.tab=0 and http://wiki.servicenow.com/index.php?title=Creating_Roles#gsc.tab=0 for more information about working with users, groups, and roles in ServiceNow.

  The ServiceNow plug-in for vRealize Automation uses the following ServiceNow roles:

User	Role
System Administrator	administrator.
Catalog Admin	vrasn_catalog_admin
ITIL User	itil
End User	No required role
Approval Manager	approver_user

  These ServiceNow users must map to appropriate users in your vRealize Automation Active Directory store for the specified tenant. For each configured user that will request machines from the catalog, you must configure the email address and apply the password in the Users System Administration area in ServiceNow.

  Note Users with the ServiceNow roles described in the preceding table must map to users with similar roles in vRealize Automation. For instance, most end users would map to the basic user role within a business group. In addition, the end user could also map to the support or business group manager roles within a business group.

  Itil users can also map to basic user, support, or business group manager roles. Itil users may be more likely to be a support or business group manager.

  System admin, catalog admin, and approval manager activities do not require a mapping to a specific role in vRealize Automation. As a best practice, the user should exist in vRealize Automation for single sign on purposes using ADFS. You could, for example, have a ServiceNow system admin with any role in vRealize Automation or admin roles.

  To set up the ServiceNow users, add the roles specified in the preceding table. Verify that the email address is the same as the user set up in vRealize Automation for single sign on through ADFS.

What to do next

Open the ApprovalMgr and update the email address, then add this user to your approval managers group. The approval managers group can be an existing group or a new group. Once your ApprovalMgr is assigned to a group, add the approval groups to the vRealize Automation workflow. See "Update the vRealize Automation Workflow for Requested Items," on page 18.

Update the vRealize Automation Workflow for Requested Items

Installation of the vRealize Automation plug-in for ServiceNow creates a workflow that runs when users request vRealize Automation catalog items from ServiceNow.

The system admin can configure the **vRA Workflow for Requested Item** using the workflow editor.

At a minimum, you must assign the approval group that contains your ApprovalMgr. When users request vRealize Automation catalog items, this workflow runs, and approvals are sent to the ApprovalMgr within the approval group before the request is submitted to vRealize Automation.

Follow the steps below to use your own approval group and add it to the vRealize Automation workflow.

Procedure

1 Search for Workflow Editor in the ServiceNow navigation pane and click it.

2 Search for **vRA Workflow for Requested Item** and open it.

3 Click the menu button and select **Checkout**.

4 Double-click the Approval group stage in the workflow.

5 Click the **Edit Groups** button.

6 Search the list of groups and make the appropriate selections.

7 Lock your selection by clicking the Lock icon.

8 Click **Update**.

9 Click the menu button and select **Publish**.

Set up the Integration User

You must set up a vRealize Automation integration user. ServiceNow requires this user to import catalog items, categories, request statuses, and resources from vRealize Automation.

In order to import items, the integration users must be a business group manager within the business groups that you want ServiceNow to manage. The integration user does not require a role within ServiceNow.

Procedure

1 Log in to vRealize Automation as a business group manager.

2 Edit your business groups and assign the integration user as a business group manager.

Set Basic Configurations for the vRealize Automation Plug-in for ServiceNow

After you install the vRealize Automation plug-in for ServiceNow, and configure users and the integration user, you can complete the set up with basic configurations.

Note In some cases, 404 errors may appear in the logs after saving the basic configurations. You can ignore these errors and proceed with the client registration and configuring the scheduled imports. The errors should stop upon completion of these steps.

Prerequisites

Install the vRealize Automation plug-in for ServiceNow. See Chapter 3, “Install vRealize Automation Plug-in for ServiceNow,” on page 15.

Procedure

1 Select **Integration - vRealize Automation > Basic Configurations**.

2 Enter the appropriate settings for your vRealize Automation tenant, URL, and plug-in.

Property	Description
MIDServer Name	The name of the MIDServer that you created for use with vRealize Automation. **Note** Do not use the FQDN of the MIDServer.
Hostname	URL address for the vRealize Automation appliance.
Tenant Name	Enter the name of the vRealize Automation tenant that you configured with ADFS applied. Only one tenant name is supported.
Integration User Username	The integration user name. The integration user must be a business group manager in all business groups. The integration user does not require a role in ServiceNow.
Integration User Password	The integration user password.
Import Catalog Items	Select **Yes** to import the vRealize Automation catalog.
Import Resources and CMDB	Select **Yes** to import vRealize Automation resources that end users own, and to import CMDB items for the itil user.
Import Request Statuses	Select **Yes** to import Request Statuses from Items.
Log Verbosity	Defines the error logging level. Levels are info, error, debug, and warning.
Report errors to Email Address	Email address to use for error reports.

3 Click **Save**.

Register the Plug-in for ServiceNow as a vRealize Automation OAuth 2.0 Client

After setting up Basic Configurations, you must register the plug-in as a vRealize Automation OAuth 2.0 client.

To register the plug-in, you must provide user credentials to authenticate to vRealize Automation. If you plan to use the vsphere.local tenant, you can use the administrator from the vsphere.local tenant. Set administrator as the username in the Register the Plug-in as a vRealize Automation OAuth 2.0 client dialog.

A second option, described in the procedure that follows, as the system admin, is to set up a user with local user and tenant admin roles within your tenant and provide these user credentials. This option registers the ServiceNow plug-in only in the specified tenant. Providing the same tenant is set in Basic Configurations, this tenant is configured for the end users.

After providing user credentials, you are prompted to set a Client ID and Client Secret. The ServiceNow admin can choose what to set as the Client ID and Client Secret. Once set, the values are saved in the `vrasn.clientID` and `vrasn.clientSecret` properties within **Integration > vRealize Automation > System Properties**. Client ID and Client Secret are later used to get the access token of the users on login within the tenant specified in Basic Configurations.

Upon completion of the registration, you are redirected back to Basic Configurations. Client registration is a one time action. If you return to client registration, a popup indicates that it has already been set and you are redirected to the Home page. If you decide you want to redo the client registration, you can clear the Value fields of the `vrasn.clientID` and `vrasn.clientSecret` properties and return to client registration.

Prerequisites

Install the vRealize Automation plug-in for ServiceNow and complete Basic Configurations.

Procedure

1 Set up a user with local user and tenant admin roles in your tenant.

   a Point to `https://vRealize Automation Hostname/vcac`

   b Log in to the vsphere.local domain as an administrator.

   c Select your tenant.

   d Create a user on the Local Users tab.

   e Select the Administrators tab and set the user as a tenant administrator.

2 Register the vRealize Automation plug-in for ServiceNow as a vRealize Automation OAuth2 client.

   a Log in to ServiceNow as a system admin.

   b Select the **Integration > vRealize Automation** module.

   c Select Client Registration.

   d Enter the user credentials in the Register the Plug-in as a vRealize Automation OAuth 2.0 Client dialog.

   For example, if the user is jdoe@vsphere.local, enter jdoe as the user name.

   e Set the Client ID and Client Secret in the Set the Client ID and Client Secret dialog.

   You must choose what to set.

On completion, you are redirected to the Basic Configurations page.

Configuring Optional Functionality

System administrators can configure additional functionality that enhance the default feature set of the vRealize Automation plug-in for ServiceNow

- Configure Resource Mappings on page 21

  As a system admin, you can configure the existing resource mappings so that the vRealize Automation Resource Types map to CMDB classes of your choosing. You must also update the payload, which maps the vRealize Automation resource data to the CMDB class fields, so that the data from vRealize Automation resources is imported into the appropriate fields in the new CMDB class.

- Set up Relationships Between Deployments and Machines on page 22

  As a system admin, you can configure relationships between resources, for example, to see what applications are linked to what machines and vice versa. The relationships you configure depend on your resource mappings.

- Rename vRealize Automation Modules and Context Menus on page 22

  You can rename vRealize Automation catalog, resource modules, and context menus.

- Update vRealize Automation Categories to Use in the Service Catalog on page 23

  Categories imported to ServiceNow are automatically linked to the vRealize Automation catalog. You can update these categories if you want to view them from the Service Catalog. You can also update them with an icon and description for a similar look and feel to other categories.

- Add Field IDs to the Exclusion List on page 23

  In some cases, unwanted fields may appear on the request form for end users. The system admin can add the field IDs to the exclusion list so that end users do not see those fields.

- Add Worknotes to See vRealize Automation Request Statuses and Failures in ServiceNow Requested Items on page 25

  You can add worknotes to requested items in ServiceNow to view status and failure information for those items. After adding appropriate worknotes, you can view the worknote information in the applicable requested item automatically with five minute updates.

Configure Resource Mappings

As a system admin, you can configure the existing resource mappings so that the vRealize Automation Resource Types map to CMDB classes of your choosing. You must also update the payload, which maps the vRealize Automation resource data to the CMDB class fields, so that the data from vRealize Automation resources is imported into the appropriate fields in the new CMDB class.

Once configured, newly provisioned resources are imported into the new CMDB class. All previously imported resources remain in the old CMDB class. You can import existing resources into the new CMDB class, but the CMDB items will reside in both classes. To avoid this situation, you should decide what mappings you want before pulling in the resources.

There is also an option to create a new resource mapping as the system admin. You must specify a valid vRealize Automation resource type, CMDB class, and payload to successfully import these resources.

Prerequisites

- Determine the vRealize Automation resource type to which you wish to map.
- Determine the data within the vRealize Automation resource schema to which you wish to map.

Procedure

1 Select **Configuration > CI Class Manager** and open the configuration item you want to map

  Note the class name in the **Name** field. You will need it when editing your resource mapping.

2 Open the fields within the configuration item you want to map to vRealize Automation data. Take note of the Column Name field. This will be used when you edit the payload of the resource mapping.

3 Select **vRealize Automation > Integration > Resource Mappings**

4 Select an existing resource mapping.

5 Edit the class name and resource type as appropriate.

6 Edit the payload sections

Payload Section	Description
CI_Details	The right-hand side reflects the name of the field on the ServiceNow form; the left-hand side reflects the vRealize Automation Resource schema key
Relationships	The right-hand side reflects the name of the field on the ServiceNow form; the left-hand side reflects the vRealize Automation Resource schema key
resourceData	The first key-value pair comes from thevRealize Automation resource schema. The second key-value pair maps the value from the first key-value pair with the ServiceNow field. The third key-value pair maps the value of the ServiceNow field with the value "value.value" from the dot walk of the vRealize Automation Resource schema.
Software_installation	Ignore, currently a placeholder only.

7 Click **Submit** or **Update**.

8 Run the importResourcesAndCMDB scheduled import.

If you do not clear the value field in the ResourcesAndCMDB property, only the newly provisioned resources are imported into the class in the new mapping. Resources in old classes prior to changing a resource mapping remain in that class. If you clear the value field in the ResourcesAndCMDB property, the newly provisioned resources and the resources provisioned prior to a changed mapping are imported into the class in the new mapping.

Set up Relationships Between Deployments and Machines

As a system admin, you can configure relationships between resources, for example, to see what applications are linked to what machines and vice versa. The relationships you configure depend on your resource mappings.

If you use the default resource mappings, you can configure a relationship between the application and machine.

Procedure

1 Select **Configuration > Relationships > Suggested Relationships**

2 Create a parent relationship with the following:

- Application as Base Class
- Hosted on (parent) as Relationship
- Global as Application
- VMware Virtual Machine Instance as Dependent Class

3 Create a child relationship with the following:

- VMware Virtual Machine Instance as Base Class
- Hosts (child) as Relationships
- Global as Application
- Application as Dependent Class

4 Run the importResourcesAndCMDB scheduled import.

If you do not clear the value field in the ResourcesAndCMDB property, only the newly provisioned resources will have the relationship. Resources imported before the relationship was created are not updated with the relationship. If you clear the value field in the ResourcesAndCMDB property, the newly provisioned resources and the resources provisioned prior will have the new relationship.

What to do next

You can view the relationship from an application or a machine.

1 Select **Configuration > Applications or Configure > VMware > Virtual Machine Instances**

2 Select a resource imported from vRealize Automation.

3 In Related Items, click the **Show dependency views** button.

Rename vRealize Automation Modules and Context Menus

You can rename vRealize Automation catalog, resource modules, and context menus.

Procedure

1 Log in as a system admin and edit the vRealize Automation modules in ServiceNow Self Service.

   a Select **System Definition > Modules**.

   b Run a title search for vRealize Automation Catalog or vRealize Automation Resources.

   c Select the module that you want to rename.

   d Change the title as appropriate and click **Update**.

   The module displays the new title in Self Service upon refresh.

2 Edit the vRealize Automation context menu when requesting catalog items.

   a Select **Catalog Definitions > Maintain Catalogs**.

   b Select the catalog that you want to rename.

   c Change the title as appropriate and click **Update**.

   The header for catalog items displays the new name upon refresh.

Update vRealize Automation Categories to Use in the Service Catalog

Categories imported to ServiceNow are automatically linked to the vRealize Automation catalog. You can update these categories if you want to view them from the Service Catalog. You can also update them with an icon and description for a similar look and feel to other categories.

Procedure

1 Select **Catalog Definitions > Maintain Categories**.

2 Search and view by name categories imported from vRealize Automation.

3 Change the Catalog field to Service Catalog.

4 Add an appropriate icon and description for a similar look and feel to other categories.

5 Click **Update**.

Upon logout and subsequent login, the category is available for addition to the Service Catalog.

Note Newly created catalog items might not be imported into ServiceNow if the category is linked to the Service Catalog. To import them, link the category back to the vRealize Automation catalog, import it, then link the category back to the Service Catalog.

Add Field IDs to the Exclusion List

In some cases, unwanted fields may appear on the request form for end users. The system admin can add the field IDs to the exclusion list so that end users do not see those fields.

You can retrieve field IDs for any given field from the catalog item schema using an API tool such as postman.

Procedure

1 Launch the postman extension in Chrome.

2 Log in as the relevant user in Chrome.

   This automatically supplies the cookies for the user.

3 Retrieve the Bearer Token for this user.

For example:

```
POST    https://vRealize Automation hostname/identity/api/tokens
    Header : Content-Type with Value : application/json
    body as raw and select JSON option.  Enter user and tenant credentials in the body:
{"username":"_username","password":"_password","tenant":"_tenant"}
```

Click **Send** to return the Bearer Token.

4 Locate the relevant catalog items by getting the entitled catalog items of the user.

a Run a query to get the catalog items.

```
GET    https://vRealize Automation hostname/catalog-
service/api/consumer/entitledCatalogItems?page=1&limit=20
    Header: Content-Type with Value : application/json
    Header : Authorization with Value: Bearer <token from step 3>
```

b Click **Send** to return to the schema with all of the catalog items to which the user is entitled.

c Copy and paste the schema into `codebeautify.org/jsonviewer` as JSON Input.

d Click Beautify and use tree view.

e Search for the catalog item by name and copy the catalog item ID specified by the `id` attribute.

5 Locate the field IDs by getting the catalog item schema using the catalog item ID.

a Run a query to get the catalog item schema.

```
GET    https://vRealize Automation hostname/catalog-
service/api/consumer/entitledCatalogItems/<catalog item id from step 4>/requests/schema
    Header: Content-Type with Value : application/json
    Header : Authorization with Value: Bearer <token from step 3>
```

This returns catalog item schema with all the fields that appear on request forms.

b Copy and paste the schema into `codebeautify.org/jsonviewer` as JSON input.

c Click Beautify and use tree view.

d Search the Catalog Item field name to locate the Catalog Item field IDs that you want to hide from the request form.

6 Add the field IDs to the exclusion list.

a Log in to ServiceNow as a system admin.

b Select **Integration > vRealize Automation > System Properties**

c Click `vrasn.exclusionList`.

d Append field IDs in the **Value** field to the existing field IDs using a comma separated list.

e Click **Update**.

To view the change, clear the value in the `ResourcesAndCMDBImportLastRunTime` property and then run the importCatalogItems scheduled import.

Add Worknotes to See vRealize Automation Request Statuses and Failures in ServiceNow Requested Items

You can add worknotes to requested items in ServiceNow to view status and failure information for those items. After adding appropriate worknotes, you can view the worknote information in the applicable requested item automatically with five minute updates.

To view updated status information, run the RequestStatus schedule import before the update occurs.

ServiceNow Status	vRealize Automation Status
Pending	pending_pre_approval
Work in Progress	in_progress
Closed Complete	successful
Closed Incomplete	failed

Procedure

1 Log in to ServiceNow as a system admin.

2 Select **Self Service > Requested Items**

3 Select the requested item of the catalog item that you selected.

4 Select **Configure > Form Layout**

5 Add `Activities (filtered)` to the selected list.

6 Click **Save**.

End users can view Request Statuses and Failures from vRealize Automation in their requested items in ServiceNow.

Configure and Run Scheduled Import Jobs

You must configure and run scheduled import jobs for the vRealize Automation ServiceNow plug-in in order to gain access to catalog items and resources.

You must manually execute scheduled jobs to import the catalog and resources. Though there is a default schedule for running jobs, you should edit the schedule time in each import according to your needs as you execute each job. For example, you might want to import catalog items every 10 minutes for high provisioning use.

The plug-in provides scheduled imports with the following functions. Scheduled imports should be configured and run in the order shown in the table.

Scheduled Import	Description
vRealize Automation-AuthGenerator	Authenticates the integration user so that the other scheduled imports can be run.
vRealize-Automation-ImportServicesAsCategories	Imports Services from vRealize Automation into ServiceNow as categories.
vRealize-Automation-ImportCatalogItems	Imports catalog items from vRealize Automation into ServiceNow as catalogs.
vRealize-Automation-ImportStorageReservationPolicies	Imports storage reservation policies displayed in request forms.

Scheduled Import	Description
vRealize-Automation-ImportResourcesAndCMDB	Imports deployments and machines from vRealize Automation into ServiceNow so that end users can view the resources they own, and so that itil can view them in CMDB as applications and virtual machine instances.
vRealize-Automation-ImportRequestStatus	Imports request statuses from vRealize Automation requests into requested items.
vRealize-Automation-QueueDelete	Deletes the scheduled import queues that are older than the interval specified.
vRealize-Automation-ReconcileCMDB	Updates deployments and machines in ServiceNow that have been destroyed in vRealize Automation. End users will no longer see these deployments and machines in the ServiceNow **Self Service > vRealize Automation Resources** page. Itil users will still see the resources in the appropriate CMDB classes, but the status is set to Retired.

Procedure

1 Configure the polling frequency for the scheduled imports.

The default polling interval for resources is five hours. For most deployments, a smaller interval is appropriate.

a Log in as the system admin.

b Select **Integration > vRealize Automation**.

c Click the applicable job name to open the scheduled import.

d Change the Repeat Interval in Days, Hours, Minutes, and Seconds.

e Click **Update**.

2 Run scheduled jobs in the order shown in the table. Ensure that each job is complete before starting the next one. Completed jobs are shown as `processed` in the Scheduled Import Queue.

For each job, complete the following steps before proceeding to the next job.

a Select **Integration > vRealize Automation > Scheduled Imports**.

b Click the **Scheduled Imports** link for the apporpriate job based on the order shown in the table.

c Click the **Execute Now** radio button in the upper right hand corner to run the script.

Completed jobs are shown as processed in the Scheduled Import Queue. Click the Updated column of the Scheduled Import Queue to refresh. The last updated time of the corresponding properties for these scheduled imports is also updated.

What to do next

Configure the **vRealize Automation Catalog** or the **Service Catalog** to view categories. Choose the catalogs that you want end users to use for provisioning requests.

1 Log in as the catalog admin or system admin.

2 Select the **vRealize Automation Catalog** or **Service Catalog**.

3 Select the plus sign in upper right corner to add vRealize Automation services, known as categories in ServiceNow, for provisioning.

4 Highlight the categories in the center pane and select **Add here**.

Add vRealize Automation Categories to the Catalog

The system admin or catalog admin must choose whether to display categories within vRealize Automation Catalog menu item, or within Service Catalog alongside whatever else they use.

By default, catalog items are linked to the vRealize Automation Catalog. If you want them to appear in the Service Catalog, you must update the catalog item to link to the Service Catalog.

Prerequisites

Configure and run scheduled import jobs.

Procedure

1 Log in as the catalog admin or system admin.

2 Select the **vRealize Automation Catalog** or **Service Catalog**.

3 Select the plus sign in upper right corner to add vRealize Automation services, known as categories in ServiceNow, for provisioning.

4 Highlight the categories in the center pane and select **Add here**.

Troubleshooting the vRealize Automation plug-in for ServiceNow

There are some basic checks you can implement if you encounter issues with the vRealize Automation plug-in for ServiceNow.

Deactivate the Plug-in

You may need to deactivate the plug-in to facilitate troubleshooting of ADFS or plug-in issue.

1 Log in as a system administrator.

2 Click System properties.

3 Locate the `vrasn.deactivate.plugin` property, and set it to True.

To re-active the plug-in, navigate to the list page of system properties in ServiceNow located at `https://msbuvrasn.service-now.com/sys_properties_list.do`, and then change the `vrasn.deactivate.plugin` property value to False.

If the plug-in stops working for some reason, refer to the following guidelines to troubleshoot.

- Verify that the status of your MIDServer is UP and Validated.

  Note Validated applies only to the Helsinki release.

- Verify that you can log in to the default vRealize Automation tenant using the administrator@vsphere.local account.

If imported catalog items are not displayed in the catalog, refer to the following guidelines to troubleshoot.

- Verify that you imported the catalog items after you imported the services and the catalog. If not, remove the imported items and re-import the services and catalog. Then, re-import the catalog items.

Log Errors

In some cases, 404 errors appear in the logs after saving the basic configurations. If you observe such errors, proceed with client registration and configuring the scheduled imports. The errors should stop upon completion of these steps. Make sure to execute the scheduled imports in the order specified.

Importing Catalog Items and Resources

Typically, importing catalog items, categories, and resources occurs simply by executing the appropriate scheduled import.

In some cases, you may need to clear the Value field of the corresponding property in **Integration > vRealize Automation > Properties** and update the property prior to executing the appropriate scheduled import. For example, this may apply when an existing catalog item or resource in ServiceNow has been changed within vRealize Automation.

Using the vRealize Automation Plug-in for ServiceNow

4

The vRealize Automation plug-in for ServiceNow supports levels of functionality for several different users.

System and Catalog Admin Functions

The following table outlines functions available to the system and catalog admin roles.

Integration - vRealize Automation page	System Admin	Catalog Admin	ServiceNow Function
Basic Configurations	Yes	Yes*	* A catalog admin cannot deactivate the plugin. Only the system admin can deactivate the plugin through the Activate the Plugin setting. See "Set Basic Configurations for the vRealize Automation Plug-in for ServiceNow," on page 18.
Scheduled Imports	Yes	Yes*	* Catalog admins have permission to execute the scheduled imports manually. But they do not have permissions to update the polling interval. Only the system admin can update the polling interval. See "Configure and Run Scheduled Import Jobs," on page 25.
System Properties	Yes	No	Catalog admins cannot view this page. System admins can view a wide range of system properties for this plug-in. Some of these correspond to the properties set on the Basic Configurations page. Others correspond to properties set on other pages by the system admin or catalog admin. System admins should not need to make changes directly to the system properties.
Properties	Yes	Yes*	■ RequestStatusImporttLastRunTime - Updated when ImportRequestStatuses scheduled import runs ■ ResourcesAndCMDBImportLastRunTime - Updated when ImportResourcesAndCMDB scheduled import runs ■ ServicesAsCategoriesImportLastRunTime - Updated when ImportServicesAsCategories scheduled import runs ■ CatalogImportLastRunTime - Updated when ImportCatalogItems scheduled import runs ■ AuthToken - Updated when AuthGenerator scheduled import runs * Catalog admins can view when the properties were last updated. But they cannot clear the **Value** field when the scheduled imports are not running. Only the system admin can clear the **Value** field. Clearing the **Value** field in properties may be needed depending on changes made to existing catalog items or resources in ServiceNow or in vRealize Automation.
Scheduled Import Queues	Yes	Yes	Once a scheduled import is triggered automatically or manually, ServiceNow processes the import in the form of queues. When an import is completed, each queue changes from a ready to a processed state.

Integration - vRealize Automation page	System Admin	Catalog Admin	ServiceNow Function
Resources Mappings	Yes	Yes*	There are two default mappings between ServiceNow CMDB classes and vRealize Automation resource types. The mapping determines the CMBU class where users can view the CMDB items. ■ `cmdb_ci_vmware_instance` - vRealize Automation Resource Type: `infrastructure.Virtual` CMDB Item in Configuration Module: **VMware > Virtual Machine Instances** ■ `cmdb_ci_appl` - vRealize Automation Resource Type: `composition.resource.type.deployment` CMDB Item in Configuration Module: **Applications** Catalog admins can only view resource mappings. System Admin can configure resource mappings. See "Configure Resource Mappings," on page 21.
Client Registration	Yes	No	Catalog admins cannot view this screen. Client registration is a one time event completed by the system admin to register the VMware Identity Manager client. See "Register the Plug-in for ServiceNow as a vRealize Automation OAuth 2.0 Client," on page 19.
Logs	Yes	Yes	Depending on the log verbosity set in Basic Configurations, you can see Debug, Info, Error, and Warning logging information related to this plugin.

Logging In

As a best practice, set up your users in both systems for single sign through ADFS. These users access `https://servicenowinstance/navpage.do` and are redirected to ADFS login. Upon login they are directed to the ServiceNow landing page.

Users in vRealize Automation that are not in ServiceNow can access `https://vRealizeAutomationSystem` and are redirected to ADFS login. Upon login they are redirected to the vRealize Automation landing page.

Approving or Rejecting Requested Items

Users with the approver_user role that are part of the approval group specified in vRA Workflow for Requested Items can approve or reject approvals. By default, all vRealize Automation catalog items requested from ServiceNow are sent for approval to the Approval Manager. If approved, the request is submitted to vRealize Automation. If rejected, the request is not submitted to vRealize Automation. Day 2 actions on resources are not sent for approval and so the request is submitted to vRealize Automation.

This chapter includes the following topics:

Viewing Resources and Performing Entitled Day 2 Actions within CMDB

Users with the Itil role can view CMDB items within the Configuration module depending on the resource mapping configuration.

By default, you can view vRealize Automation deployments by selecting **Applications**, and vRealize Automation Virtual Machines by selecting **VMware > Virtual Machine Instances**.

Users with the Itil role can perform actions on these resources by viewing the details of the deployments or machines and clicking on the **Action** button. Itil users see only the actions they are entitled to perform on that resource. Unsupported actions are not visible.

When you click an action, a popup with an `Action has been Submitted` message appears. Also, the request is submitted to vRealize Automation and the action is performed on the resource.

Viewing Resources and Performing Entitled Day 2 Actions within Self-Service

End users can view their resources from the vRealize Automation Resources menu item.

End users can perform actions on these resources by viewing the details of the relevant resource and clicking the **Actions** button. They see the actions to which they are entitled.

End users can view their own deployments and machines from the **Self Service > vRealize Automation Resources** menu item. They can perform actions on their resources by viewing the details of the deployments or machines and clicking the **Action** button. End users will see only the actions they are entitled to perform on that resource. Unsupported actions are not visible.

When you click an action, a popup message appears stating that an Action has been Submitted. The request is submitted to vRealize Automation which performs the action on the resource.

Viewing and Requesting Entitled Catalog Items within Self-Service

End users can view categories by selecting **Self Service > vRealize Automation Catalog** depending on where the system admin or catalog admin added the categories.

For example, if the category is added to the Service Catalog, end users can see that category in their Service Catalog. If end users are entitled to catalog items within that category, they can see catalog items within that category in the Service Catalog.

When requesting a catalog item, users can enter valid values similar to the fields in vRealize Automation request forms. vRealize Automation catalog items can be added to the cart. The quantity in the cart reflects the number of catalog item deployments that you are requesting.

Once the request is submitted, users can view requested item to see updates to request status or reasons for provisioning failures from vRealize Automation providing the system admin has added work notes for that requested item.

Update the Default Catalog Items Display Number

The number of catalog items in a user's cart is currently limited to five by default. ServiceNow administrators can change the default quantity of displayed catalog items.

Prerequisites

Log in to ServiceNow as a system administrator.

Procedure

1 Search for Tables in the ServiceNow navigation pane and select the heading.

2 Select Tables from the System Definition Category.

3 Select the `sc_cart_item` in the filter box on the right side of the page.

4 Select the `sc_cart_item` in the table and click the **Item** link.

5 Click the **Quantity** link on the Columns tab.

The Quantity definition with the default Choices tab will appear selected at the bottom of the page.

6 Select a **New** action from Choices to add a new entry that specifies the default catalog items number.

Supported and Unsupported Functionality

5

The vRealize Automation plug-in for ServiceNow provides access to some vRealize Automation Day 2 actions.

Supported Versions

The vRealize Automation plug-in for ServiceNow works only with vRealize Automation 7.3, and is available only for the ServiceNow Helsinki and Istanbul releases. Also, the ADFS configuration described herein uses ADFS 2.0. Newer versions of ADFS have not been tested.

Day 2 Actions for vCenter Resources

Day 2 actions with approvals triggered in ServiceNow are currently not supported. When you submit a Day 2 action, the request is sent to vRealize Automation and executed.

Day 2 actions that require input from the user are currently not supported from ServiceNow. For example, Change Lease and Change Owner deployment actions that require input from the user are unsupported. Likewise, the Reconfigure machine action requires user input and unsupported.

Day 2 actions related to connecting to machines are not supported from ServiceNow. For example, Connect using RDP is unsupported.

Unsupported Day 2 actions are not visible from ServiceNow.

The following table outlines Day 2 actions that are available to end users and itil users from ServiceNow.

	Name	Resource Type	Plug-in Support
Deployment Actions			
	Change Lease	Deployment	No
	Change Owner	Deployment	No
	Scale Out	Deployment	No
	Scale In	Deployment	No
	Destroy	Deployment	Yes
	Expire	Deployment	Yes
Machine Actions			
	Re-provision	Machine	No
	Install Tools	Machine	Yes
	Suspend	Machine	Yes
	Power On	Machine	Yes

	Name	Resource Type	Plug-in Support
	Disassociate Floating IP	Machine	No
	Power Off	Machine	Yes
	Cancel Reconfigure	Machine	No
	Shutdown	Machine	Yes
	Execute Reconfigure	Machine	No
	Power Cycle	Machine	No
	Change Lease	Machine	No
	Reconfigure	Machine	No
	Reboot	Machine	Yes
	Expire	Machine	Yes
	Unregister	Machine	No
	Get Expiration Reminder	Machine	No
	Export Certificate	Machine	No
	Connect using RDP	Machine	No
	Connect using ICA	Machine	No
	Connect using SSH	Machine	No
	Connect using Virtual Desktop	Machine	No
	Connect to Remote Console	Machine	No
	Connect using VMRC	Machine	No
	Connect using Console Ticket	Machine	No
	Associate Floating IP	Machine	No
Virtual Machine Actions			
	Create Snapshot	Virtual Machine	No
	Revert to Snapshot	Virtual Machine	No
	Destroy	Virtual Machine	Yes
	Delete Snapshot	Virtual Machine	No
	Unregister VDI	Virtual Machine	No
	Register VDI	Virtual Machine	No

Day 2 Actions for Amazon Resources

The following Day 2 actions are supported for Amazon resources: Power On, Power Off, Reboot, Shutdown, and Destroy.

Requesting Catalog Items from Non-vCenter Endpoints

AWS and vCenter catalog items requesting single machines and applications are supported from the ServiceNow catalog. Requesting non vCenter catalog items such as Azure catalog items from the ServiceNow catalog is not currently supported. Likewise, requesting XaaS catalog items is not supported.

Requesting vCenter Catalog Items on Behalf of Users

Requesting catalog items, as a business group manager or support user, on behalf of users from the same business group is not currently supported.

Requesting Catalog Items with Custom Properties

Requesting vCenter catalog items with custom properties of the following field types with static values are supported from ServiceNow - textbox, checkbox, dropdown, textarea, yes/no, Date time picker.

Requesting vCenter catalog items with custom properties of the following field types are not supported from ServiceNow - Slider, spinner, hyperlink, securestring.

Requesting vCenter catalog items with custom properties with external values are not supported from ServiceNow. For example, custom properties that involve vRealize Orchestrator actions.

Note The custom properties option is not available for Amazon Web Service blueprints on the ServiceNow request form. As a workaround, you can define properties and values on the vRealize Automation blueprint.

Other Unsupported Functionality

ServiceNow does not display machine details or deployment details Amazon Web Service vRealize Automation resources. In addition, ServiceNow does not display the Security Groups option for VPC and non-VPC catalog items.

ServiceNow lists all Amazon virtual machine instances unlike vRealize Automation which lists only those instances selected in the applicable blueprint. If a user selects an instance that is not part of the vRealize Automation blueprint, provisioning from ServiceNow fails with an error. Users must select only instances that are part of the applicable vRealize Automation blueprint.

The following functions are also unsupported.

- Catalog Item and Service/Category icons.
- The machine instances field with ServiceNow request forms.

Note All sub-nets are currently visible to users.

Index