

VMware vSphere Automation SDK for REST 6.7 Release Notes

VMware vSphere Automation SDK for REST 6.7 | 17 APR 2018

Check for additions and updates to these release notes.

Overview

The VMware vSphere Automation SDKs provide support for your client application infrastructure with services to perform management operations in your vSphere environment. The vSphere Automation SDK for REST also contains samples to demonstrate how to use the new APIs.

The version 6.7 SDK enables programmatic access to the following services:

- Service discovery (Lookup Service)
- Authentication (Single Sign-On)
- Session management
- Tagging
- Content Library
- Virtual Machines
- vCenter Server Appliance management
- vCenter Server Appliance and Platform Services Controller appliance deployment

Note: Single Sign-On authentication is available through the VMware vCenter Single Sign-On API and the vSphere API. Service discovery is available through the Lookup Service API. This feature can be accessed using the SOAP API mechanism shown in the SDK samples.

Distribution Kit

You can clone and download the vSphere Automation SDK for REST distribution kit from the <https://github.com/vmware/vsphere-automation-sdk-rest>.

What's New

The vSphere Automation SDKs for vSphere 6.7 includes new APIs for:

- Storage Policy
- Guest Ops
- vCenter Server Appliance and Platform Services Controller appliance deployment

For information about the new APIs and samples, see the vSphere Automation repositories at GitHub.

Caveats and Limitations

The vcenter API includes the following methods that have known issues and might be removed in a future version. It is advised that these APIs are not invoked:

- `DeploymentType.reconfigure`
- `PscRegistration.repoint`
- `Upgrade.cancel`
- `Deployment.rollback`

Known Issues

- **Unauthenticated exception following long-running operation**

After an API client completes a long-running operation, such as an upload to the content library, the next operation might fail with an "Unauthenticated exception" message. This happens if the long running operation did not complete within the lifetime of the authentication session.

Workarounds:

- Keep the session alive by issuing short operations on another thread until the long running operation completes.
 - Increase the session length using the VMware vSphere Web Client. Select **Administration > System Configuration > Services > vAPI Endpoint > Manage > General**, and increase the value for the Maximum session idle time.
- **API Explorer does not work with the Internet Explorer browser**

The API Explorer does not load properly in Internet Explorer 11. The browser displays a blank page.

Workaround:

Use a different browser, such as Firefox, Chrome, or Edge.

- **API Explorer unsupported operations**

The "Try it Out" feature in the API Explorer is not supported for some operations.

When you try the following operations in API Explorer, they yield error messages:

- <https://vcip/rest/com/vmware/vcenter/inventory/datastore?-action=find>
- <https://vcip/rest/com/vmware/vcenter/inventory/network?-action=find>
- <https://vcip/rest/com/vmware/vcenter/ovf/import-flag>

- **Enabling certificate validation**

The samples in the vSphere Automation SDK for REST do not enable certificate validation for service endpoints by default. To enable certificate validation, modify the code that sets request options. Where the flag `rejectUnauthorized` is set to `false` in the samples, set the value to `true` instead.

If the service endpoint uses an untrusted certificate, you have two ways to use it in the client:

- Download the certificate authority's root certificate, using a Web browser connected to the service endpoint, and import it into your client machine certificate store.
- Modify the sample code to specify a certificate file in the request options.

The following code extract shows the second way:

```
function makeAuthRequestOptions(ssoConnectionInfo, requestXml) {  
  
  return {  
  
    host: ssoConnectionInfo.host,  
  
    path: ssoConnectionInfo.path || '/sts/STSService/vsphere.local',  
  
    port: ssoConnectionInfo.port || 443,  
  
    method: 'POST',  
  
    rejectUnauthorized: true, // was: false to ignore server SSL validation.  
  
    ca: fs.readFileSync('/path/to/downloaded/root.cer'), // VMCA root certificate from PSC  
  
    requestCert: true,  
  
    agent: false,  
  
    headers: {  
  
      'Content-type': 'text/xml; charset="UTF-8"',  
  
      'Content-length': requestXml.length,  
  
      'User-Agent': 'VMware/jsSample',  
  
      'Connection': 'keep-alive',  
  
      'SOAPAction': "http://docs.oasis-open.org/ws-sx/ws-trust/200512/RST/Issue"  
  
    }  
  
  }  
  
}
```