

vSphere Web Services SDK Developer's Setup Guide

21 SEP 2023

VMware vSphere 8.0

vCenter Server 8.0

VMware ESXi 8.0

You can find the most up-to-date technical documentation on the VMware by Broadcom website at:

<https://docs.vmware.com/>

VMware by Broadcom

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

Copyright © 2012-2023 Broadcom. All Rights Reserved. The term “Broadcom” refers to Broadcom Inc. and/or its subsidiaries. For more information, go to <https://www.broadcom.com>. All trademarks, trade names, service marks, and logos referenced herein belong to their respective companies. [Copyright and trademark information](#).

Contents

About This Book 5

1 What is the vSphere Web Services SDK 7

What you need to know for the vSphere Web Services SDK 7

Programming Language Support in the vSphere Web Services SDK 8

Types of Applications That You Can Build Using This SDK 8

How You Can Download the vSphere Web Services SDK 9

Sample Authentication with Single Sign-On Configurations 9

What files are in the vSphere Web Services SDK package 10

SDK Version Support and Limitations of the ESXi API 11

2 Set Up to Develop in Java with the vSphere Web Services SDK 12

Java Development Requirements for the Web Services SDK 12

Set Up for Java Development for the Web Services SDK 13

Software Downloads for the Web Services SDK 13

Set Up for Development Using JAX-WS with the Web Services SDK 13

Batch Files and Shell Scripts for Building and Running Samples in the Web Services SDK 14

Import Server Certificates into the Java Keystore for the Web Services SDK 15

Generating Stubs and Compiling Classes for the Web Services SDK 16

Precompiled JAX-WS Samples in the Web Services SDK 16

Use the Included Build Scripts in the Web Services SDK 16

Running the Web Services SDK SimpleClient Sample Application to Validate Setup 17

Run a Sample Application Using the Provided Scripts in the Web Services SDK 18

3 vSphere Server Certificates 20

Secure Client-Server Communications 20

Simplified Security Setup for Development Environment 20

Obtaining Server Certificates 21

Obtain Certificates Using the vSphere Client 21

Updating the Active Directory Group Policy to Accept Certificates 22

4 Endpoint Configuration for HTTP 24

Modifying Service Endpoint Configurations to Support HTTP 24

HTTP Configuration for Web Services API Endpoint 25

HTTP Configuration for Web Services API Endpoint on ESXi or vCenter Server for Windows 25

HTTP Configuration for Web Services API Endpoint on vCenter Server Appliance 27

HTTP Configuration for vSphere Automation API Endpoint 29

About This Book

This book, the *vSphere Web Services SDK Developer's Setup Guide*, provides information about setting up your development environment to use the VMware® vSphere Web Services SDK.

VMware provides several different APIs and SDKs for various applications and goals. This book provides information about using the vSphere Web Services SDK for developers who are interested in creating client applications for managing VMware® vSphere components available on VMware ESXi and VMware vCenter Server systems.

To view the current version of this book as well as all VMware API and SDK documentation, go to http://www.vmware.com/support/pubs/sdk_pubs.html

Revision History

This guide is revised with each release of the product or when necessary. A revised version can contain minor or major changes. The Revision History summarizes the significant changes in each version of this guide.

Table 1-1. Revision History

Revision	Description
21 SEP 2023	vSphere 8.0 Update 2 release. <ul style="list-style-type: none">■ Minor changes for search engine optimization.
11 OCT 2022	vSphere 8.0 release. <ul style="list-style-type: none">■ .NET content removed.
05 OCT 2021	<ul style="list-style-type: none">■ Update to JDK 11 in the vSphere Management SDK.■ Update certificate procedure.
12 APR 2021	VMware has rebranded the My VMware portal as VMware Customer Connect. We have updated this document accordingly.
09 Mar 2021	vSphere 7.0 Update 2 release, with Java 11 work-around.
06 Oct 2020	vSphere 7.0 Update 1 release.
02 Apr 2020	vSphere 7.0 release: Java 1.7 no longer supported.
17 Apr 2018	Minor updates for vsphere 6.7.
05 Nov 2016	Update and restructure procedures for modifying service endpoints with vSphere 6.5. Simplify process of building C# DLLs and samples.
12 Mar 2015	vSphere 6.0 release. Changed destination directory for C# DLLs.

Table 1-1. Revision History (continued)

Revision	Description
20 Feb 2014	Corrected instructions for modifying reverse proxy configuration.
04 Dec 2013	Clarified location of Web Services SDK.
01 Oct 2013	Revised C# setup instructions to reflect simplified procedure in 5.5 release and use new tools. Corrected path to Java sample. Updated Java version. Fixed minor typographical errors in code.
09 Sep 2012	Removed Axis support for 5.1 release. Made more corrections and expansions to C# instructions.
17 Nov 2011	Corrected setup instructions for C# stubs.
24 Aug 2011	Updated for vSphere 5.0 (included information on using JAX-WS bindings).
13 Jul 2010	Minor updates for vSphere 4.1 (new WSDL file configuration, example syntax).
07 May 2009	Revised release of the <i>vSphere Web Services SDK Developer's Setup Guide</i> for vSphere Web Services SDK 4.0. Server-certificate setup information is located in the reference section. Changed directory name for WSDLFILE environment variable.
29 Nov 2007	Initial release of <i>vSphere Web Services SDK Developer's Setup Guide</i> for VMware Infrastructure SDK 2.5.

Intended Audience

This book is intended for anyone who wants to develop applications using the VMware vSphere Web Services SDK. vSphere Web Services SDK developers typically include software developers creating client applications using Java and targeting VMware vSphere.

Document Feedback

VMware welcomes your suggestions for improving our documentation. Send your feedback to docfeedback@vmware.com.

What is the vSphere Web Services SDK

1

The VMware vSphere® Web Services SDK helps you develop client applications for the VMware vSphere API. Learn how to install it in this publication.

The

vSphere Web Services SDK includes all the components necessary to work with the VMware vSphere API, including WSDL files, sample code, and libraries. With the vSphere Web Services SDK, developers can create client applications to manage, monitor, and maintain VMware vSphere components, as deployed on VMware® VMware vSphere® ESX®, ESXi™, and VMware® vCenter™ Server systems.

This *vSphere Web Services SDK Developer's Setup Guide* explains how to set up the development environment to create new applications with Java. This guide also includes information about running the sample applications included with the vSphere Web Services SDK.

Read the following topics next:

- [What you need to know for the vSphere Web Services SDK](#)
- [Programming Language Support in the vSphere Web Services SDK](#)
- [Types of Applications That You Can Build Using This SDK](#)
- [How You Can Download the vSphere Web Services SDK](#)
- [What files are in the vSphere Web Services SDK package](#)
- [SDK Version Support and Limitations of the ESXi API](#)

What you need to know for the vSphere Web Services SDK

To develop applications for the vSphere Web Services SDK requires a programming language with a SOAP toolkit. You must also understand the following concepts:

- Web services technology provides operations, also known as methods in the context of client applications. Using the vSphere Web Services SDK and your choice of programming language, you can create client applications that invoke these operations to perform the full range of server-side management and monitoring tasks.
- The Web services API is defined in Web Services Description Language (WSDL) files. The WSDL files are used by client-side Web-services utilities to create proxy code (stubs) that client applications use to interact with the server.

- Client applications invoke operations by calling proxy interface methods. The client proxy encodes an operation invocation into a SOAP message and sends it to the server. Simple Object Access Protocol (SOAP) is a programming-language neutral XML format. SOAP message translation is transparent to the developer.
- Communications between client and server occur over HTTP or HTTPS. HTTPS is a secure form of HTTP that uses SSL to encrypt client-server communications. The default is HTTPS, but you can configure the VMware vSphere Web server to support HTTP. (See [Chapter 4 Endpoint Configuration for HTTP](#).)

You should also know about basic ESXi and vCenter Server operations. See the VMware vSphere Documentation page on the VMware Web site.

Programming Language Support in the vSphere Web Services SDK

You can develop for the vSphere API in any language from which you can generate client-side stubs from Web-services WSDL files. This section describes SDK support for Java clients.

See [What files are in the vSphere Web Services SDK package](#) for additional packaging details and for some caveats about the Java samples and for specific version requirements for the JDK, the Java API for XML Web Services libraries, and the JAXB libraries.

Language/Tool Context	Java
Development environment or framework	JDK 11 (also known as J2SE 1.11).
Web-services-client application development toolset, also known as a SOAP toolkit	JAX-WS 2.3.3 and later (Java/Jakarta XML Web Services). JAXB 2.3.2 and later (Java/Jakarta XML Binding).

SOAP toolkits are readily available for Java. Developers, scripters, and administrators can also use Microsoft PowerShell or Perl with the vSphere Web Services API through toolkits that VMware provides. For more information, see <http://communities.vmware.com/community/developer>.

Types of Applications That You Can Build Using This SDK

You can use the vSphere Web Services SDK to develop system administration, provisioning, and monitoring applications for VMware vSphere systems.

The VMware vSphere Client application and VMware vSphere Web Access are two examples of client applications that were developed using vSphere API. The vSphere Client is a traditional Windows client application. Web Access is a browser plug-in that is available through the Web server port on ESXi and vCenter Server systems.

With the vSphere Web Services SDK, you can create your own client applications that automate many administration, provisioning, or monitoring tasks associated with virtual infrastructure management and operations. The following examples are operational tasks that you can automate using the vSphere Web Services API:

- Create, configure, power cycle, or suspend virtual machines explicitly or by using profiles or templates to facilitate faster provisioning.
- Create, configure, and manage virtual devices, such as virtual CD-DVD drives, virtual network interface cards, virtual switches, and other components.
- Connect, power cycle, and disconnect ESXi host systems.
- Capture the state of a virtual machine to a snapshot and restore the state of a virtual machine from a snapshot, such as in a backup application.
- Gather statistics about host system and virtual machine performance.
- Manage events generated by the server, such as those created by alarms set for specific thresholds.
- Move virtual machines between hosts automatically.
- Manage load balancing and failover through the distributed resource scheduler (VMware DRS) and high availability (VMware HA) subsystems. VMware DRS and VMware HA require vCenter Server.

This list is not comprehensive. Also, some of the operations pertain to the service as a whole, not specific hosts or virtual machines. For example, load balancing can be a service-wide operation rather than a per-host or per-virtual machine operation.

How You Can Download the vSphere Web Services SDK

The vSphere Web Services SDK is part of the vSphere Management SDK. This section tells how to access the Web Services SDK files.

You can download the vSphere Management SDK at <https://code.vmware.com>. Click the **SDKs** link to reach a landing page that has links to all vSphere SDKs. After you download and expand the vSphere Management SDK package, the Web Services SDK is in the subdirectory `SDK/vsphere-ws`. You also need the `SDK/ssoclient` subdirectory for client authentication.

Sample Authentication with Single Sign-On Configurations

You can choose to authenticate your client with vCenter Server Single Sign-On. This topic explains how to do Single Sign-On authentication with the SDK samples..

At this time, the two possible configurations are:

- vCenter Server with an embedded Platform Services Controller, which includes vCenter Single Sign-On Server, Lookup Service Server, and other features. This configuration combines all the platform services in the same installation with vCenter Server.

- vCenter Server with an external Platform Services Controller, where the platform services are installed on a different host or in a different virtual machine from vCenter Server.

You will have to provide the vCenter Single Sign-On URL explicitly in order to run samples with the second configuration. With the first configuration, there is no need to provide the vCenter Single Sign-On URL (since the vCenter Single Sign-On service is embedded in the management node) and our SDK will continue to work as before.

The SDK samples have always had the option to explicitly specify the vCenter Single Sign-On URL (whether the vCenter Single Sign-On service is running inside or outside the management node). This is useful in cases where the vCenter Single Sign-On service is deployed outside the vSphere management node like the second configuration above.

When you log in to a vCenter Single Sign-On Server, you must be in a domain that has been added as a vCenter Single Sign-On identity source. If that domain is not the default domain, you must include the domain name as part of your user name, such as, administrator@vsphere.local. To learn more about configuring the vCenter Single Sign-On Server, see vSphere Security.

What files are in the vSphere Web Services SDK package

The vSphere Web Services SDK is one of several SDKs bundled inside the vSphere Management SDK. The Web Services SDK contains the following files:

- WSDL files that define the API available on a VMware vSphere server (ESXi or vCenter Server) Web service.
- Precompiled client-side libraries (`vim.jar`, `vim25.jar`) available for test purposes that were generated from the WSDL. The vSphere Web Services API is packaged in the `vim25.jar` file and is available in the `SDK\vsphere-ws\wsdl\vim25` subdirectory.
- Sample code demonstrating common use cases associated with managing virtual infrastructure. The sample code includes compiled and ready-to-run Java class files and source code files.
- Batch files and shell scripts (`build.bat` and `build.sh`) that automate the build process for Java client applications.
- Batch files and shell scripts (`run.bat` and `run.sh`) that facilitate running the Java samples from the Windows command prompt.
- The *vSphere API Reference*, which provides language-neutral descriptive information about the VMware vSphere API and the object model, such as object type definitions, properties, and method signatures.

Complete information about setting up the environment, and about generating, compiling, and running applications is included in [Chapter 2 Set Up to Develop in Java with the vSphere Web Services SDK](#).

SDK Version Support and Limitations of the ESXi API

vSphere supports various versions, both with vCenter Server and with ESXi. The ESXi service contains some limitations not present in vCenter Server.

You can use the VMware vSphere Web Services SDK with many previous versions of VMware vSphere servers and its predecessor, VMware Infrastructure, including:

- ESXi 8.0, 7.0, 6.7, 6.5, 6.0
- vCenter Server 8.0, 7.0, 6.7, 6.5, 6.0

All versions are supported by the WSDL declarations in the `vimService.wsdl` top-level file in the `vim25` directory.

The VMware vSphere API is a Web service that runs on VMware vSphere ESXi and vCenter Server. The API exposed is the same in both products. However, vCenter Server provides the following capabilities which are not available through an ESXi Web service:

- Collecting historical performance data
- Optimizing resources, including managing distributed resources
- Enabling migration from one host system to another by using VMware vMotion
- Providing distributed resource management, including recovery, across all host systems under its control

If you attempt to invoke an operation on an ESXi system that is supported only on vCenter Server, the server returns a fault saying “not implemented” or “not supported.” For example, the ExtensionManager API is available only on VirtualCenter Server. Attempting to register an extension to an ESXi system returns a fault, “not supported.”

Set Up to Develop in Java with the vSphere Web Services SDK

2

To develop a Web Services client, you need a development environment. This chapter explains how to set up an environment to develop in Java.

Read the following topics next:

- [Java Development Requirements for the Web Services SDK](#)
- [Set Up for Java Development for the Web Services SDK](#)
- [Generating Stubs and Compiling Classes for the Web Services SDK](#)
- [Running the Web Services SDK SimpleClient Sample Application to Validate Setup](#)

Java Development Requirements for the Web Services SDK

To develop Java client applications using the VMware vSphere Web Services SDK, you need Java SE and a Java Web services development toolset.

For best results, use the Java platform Standard Edition (SE) version 11. Java SE includes both the runtime environment (JRE) and the development kit (JDK).

The Java Web services development toolset must be a SOAP implementation that can be deployed to a Tomcat server. For example, you can use the client-side libraries in JAX-WS. The JAX-WS libraries are included with the vSphere Management SDK.

You can use other client-side tools and libraries, such as IBM WebSphere and several open source implementations, such as Open JDK, with the vSphere Web Services SDK. However, only the JAX-WS client libraries were tested with this guide.

The samples archive, in `samples.jar`, includes all vSphere Web Services SDK samples. The samples include client-side stub classes generated using the JAX-WS libraries.

Note Use JDK 11 for production environments. vCenter Server supports HTTPS connections with Java 1.8 and later, but not with Java 1.7. If you need to use Java 1.7 for development work, see [Chapter 4 Endpoint Configuration for HTTP](#).

Set Up for Java Development for the Web Services SDK

Specific setup instructions depend on whether your development workstation already meets some or all of the requirements, which client-side Web service library you plan to use, and whether you plan to use the provided samples. Specific setup instructions also depend on whether your target server uses the HTTPS protocol or HTTP.

Software Downloads for the Web Services SDK

You can obtain the software you need for Java client development from the following Web sites:

- The JDK is available from <http://www.oracle.com>. The vSphere API supports connections from JDK 11.
- Obtain the VMware vSphere Web Services SDK from <https://developercenter.vmware.com>. It is included in the vSphere Management SDK package.

Set Up for Development Using JAX-WS with the Web Services SDK

The Web Services SDK provides precompiled samples that use JAX-WS libraries. The precompiled files include `vim25.jar` and `samples.jar`.

The precompiled sample programs use the `vim25.jar` client side library to access the Web Services API. The following instructions describe how to set up your environment to run sample programs. These instructions assume that the target server uses HTTPS, which is the default server configuration.

Procedure

- 1 If the JDK is not installed, create directories for the JDK and for the vSphere Web Services SDK package.

Do not use spaces in the directory names, to avoid issues with some of the included SDK batch and script files.

- 2 Install Java SE with JDK 11.
- 3 Unpack the components into subdirectories created in [Step 1](#), using the provided installer if appropriate.

The JDK uses an installation wizard. The SDK ZIP file unpacks into the directory you specify.

- Unpack with **Use folder names** selected, to maintain the organizational structure.
- On UNIX development systems, use the `unzip` command with the `-a` modifier, to ensure proper line-endings in the shell scripts. For example:

```
unzip -a VMware-vSphere-SDK-8.0.0-14379537.zip
```

- 4 (Optional) Import server-certificates and use the Java keytool utility to create a `vmware.keystore`. See [Import Server Certificates into the Java Keystore for the Web Services SDK](#) for details.

As an alternative, pass the `--ignorecert` argument at runtime to ignore server-certificate verification for any of the sample Java applications.

- 5 Create the `JAVAHOME` environment variable.

The `JAVAHOME` environment variable must be set to the root path of the Java Runtime Environment (JRE), such as `C:\Program Files\Java\jdk11.0.16_221`. The root directory of your Java installation contains `bin\javac` and other binary files needed to build the stubs and the samples.

- 6 If you are unable to use the `run.bat` or `run.sh` script to run Java samples, add the precompiled sample files, `vim25.jar` and `samples.jar`, to your system `CLASSPATH` environment variable.

To test your setup, run the Java version of SimpleClient, as described in [Running the Web Services SDK SimpleClient Sample Application to Validate Setup](#).

Batch Files and Shell Scripts for Building and Running Samples in the Web Services SDK

The vSphere Web Services SDK includes several batch files for Windows and shell scripts for Linux that facilitate building and running the sample applications.

Some of the batch files are used by other batch files. For example, `build.bat` calls the `lcp.bat` and `clean.bat` scripts. If you modify the batch files for any reason, be aware of the dependencies among them.

Filename	Description	Usage note
<code>build.bat</code> <code>build.sh</code>	Checks for environment variable <code>JAVAHOME</code> and sets <code>PATH</code> , using the <code>JAVAHOME</code> variable. Cleans up existing Java files (by calling <code>clean.bat</code> or <code>clean.sh</code>). <code>build.bat</code> sets the local classpath (by calling <code>lcp.bat</code>). Creates the <code>vim25.jar</code> , and <code>samples.jar</code> files.	Use this script to generate client stubs and rebuild all sample applications. Use the <code>-w</code> flag to recompile without regenerating stubs.
<code>lcp.bat</code>	Sets the local classpath on the workstation. Called by <code>build.bat</code> and by <code>run.bat</code> .	Optional. Use to set local classpath.
<code>run.bat</code> <code>run.sh</code>	Batch file that enables running any of the sample applications. Sets the Java <code>trustStore</code> property to the local trust store and invokes the Java runtime with the name of the application passed as a parameter.	Use this script to run any Java sample applications.
<code>clean.bat</code>	Removes any existing artifacts before building the samples, deleting Java class files in the samples packages and <code>samples.jar</code> file. Called by <code>build</code> script.	Optional. Deletes all generated source code files.

Import Server Certificates into the Java Keystore for the Web Services SDK

Import server certificates if you plan to use the HTTPS protocol and if you do not plan to use the `--ignorecert` command-line argument.

To use HTTP, rather than HTTPS, and avoid the use of certificates entirely, follow the procedure detailed in [Chapter 4 Endpoint Configuration for HTTP](#). However, using HTTPS provides better security for production environments.

The JAVAHOME environment variable must be set and added to the PATH environment variable. The certificate for each target server must be located in the `vmware-certs` subdirectory, as described in this procedure. For detailed information about server certificates, see [Obtaining Server Certificates](#).

Procedure

1 Open the Windows command prompt or Linux shell command.

2 Create the directory for the Java certificate store.

Create the directory only. The actual keystore file, `vmware.keystore`, is created during the process of importing the certificates.

Operating System	Path
Windows	C:\VMware-Certs\vmware.keystore
Linux	~/vmware-certs/vmware.keystore

3 Navigate to the directory.

For example, on Windows use the following directory:

```
cd vmware-certs\vmware
```

4 Use the Java `keytool` utility to import a certificate.

The syntax is as follows:

```
keytool -import -trustcacerts -alias server-name -file certificate-filename -keystore keystore-name
```

For example:

```
C:\VMware-Certs>keytool -import -trustcacerts -alias root -file root.cer -keystore keystore.jks
```

A prompt requesting a password for the keystore appears:

```
Enter keystore password:
```

- 5 Create a password for the keystore by entering it at the prompt.

The keystore utility displays the certificate information at the console. For example:

```
Owner: OID.1.2.840.113549.1.9.2="1183400896,564d7761726520496e632e",
CN=sdkslab-01.vmware.com, EMAILADDRESS=ssl-certificates@vmware.com,
OU=VMware ESX Server Certificate, O="VMware, Inc.", L=Palo Alto,
ST=California, C=US Issuer:
OID.1.2.840.113549.1.9.2="1183400896,564d7761726520496e632e",
CN=sdkslab-01.vmware.com, EMAILADDRESS=ssl-certificates@vmware.com,
OU=VMware ESX Server Certificate, O="VMware, Inc.", L=Palo Alto,
ST=California, C=US Serial number: 0 Valid from: Mon Jul 02 11:28:17 PDT 2007 until: Mon
Aug 31 11:28:17 PDT 2026
Certificate fingerprints:
MD5: . . .61:35:C0:C4
SHA1: 4C:...78:B2
```

At the end of the certificate information, a prompt displays a request for confirmation that the certificate is trusted:

```
Trust this certificate? [no]:
```

- 6 Type yes and press Enter to respond to the prompt and import the certificate into the `vmware.keystore` keystore.

The console displays this message:

```
Certificate was added to keystore
```

- 7 Repeat [Step 4](#) through [Step 6](#) for each target server.

Generating Stubs and Compiling Classes for the Web Services SDK

The vSphere Web Services SDK includes a set of Java archive files for the sample programs. The sample `.jar` files were created using the JAX-WS Web services libraries.

Precompiled JAX-WS Samples in the Web Services SDK

The JAX-WS samples include the `vim25.jar` and `samples.jar` files that were created using the JAX-WS libraries included with the JDK. These files are located in the `%WS_SDK_HOME%\java\JAXWS\lib` directory.

To use these precompiled libraries, see the instructions in [Running the Web Services SDK SimpleClient Sample Application to Validate Setup](#). If you modify the precompiled code, see the build instructions in [Use the Included Build Scripts in the Web Services SDK](#).

Use the Included Build Scripts in the Web Services SDK

If you modify the sample files, or need to rebuild them for any reason, you can use the `build.bat` or `build.sh` script included with the SDK. These scripts performs all necessary tasks to build the SDK files.

This task shows how to use the build scripts included with the SDK.

Prerequisites

You must install the JDK and set the `JAVAHOME` environment variable.

Procedure

- 1 Open a command prompt.
- 2 Navigate to the subdirectory containing the `build.bat` and `build.sh` files.

```
cd %WS_SDK_HOME%\java\JAXWS\
```

- 3 Run the `build.bat` (or `build.sh`) script by entering its name at the command prompt.

```
build
```

The console displays output, starting with `Generating stubs from wsdl`. In a few minutes, the process finishes. The word `Done` appears at the command prompt, as shown in the following example. The `Generating stubs from wsdl` message appears twice, because this build file generates client stubs using both sets of WSDL declarations, found in the `\vim` and `\vim25` subdirectories.

Successful Stub Generation and Compilation Using the `build.bat` Script

```
Generating stubs from wsdl
Compiling stubs.
...
Done.
C:\devprojects\visdk21\SDK\vsphere-ws\java\JAXWS>
```

Results

When the process finishes, the appropriate sample `.jar` files show the current date and time.

To compile without re-generating the stubs from the WSDL, use the `-w` flag with the build script, as follows:

```
build -w
```

You can run any of the sample applications by following the instructions in [Running the Web Services SDK SimpleClient Sample Application to Validate Setup](#)

Running the Web Services SDK SimpleClient Sample Application to Validate Setup

You can test your setup and connectivity by running one of the sample applications, such as SimpleClient. SimpleClient is a Java class that connects to the server and obtains a listing of the

top-level inventory entities, their properties, and references. You can run any of the samples using the `run.bat` (or `run.sh`) script.

If you are using stubs generated by JAX-WS, these scripts require the `JAVAHOME` environment variable to be set.

Run a Sample Application Using the Provided Scripts in the Web Services SDK

You can use the `run.bat` or `run.sh` script to run any of the Java samples. The `SimpleClient` sample is a good choice to verify that your installation is correct. The path to the source file for `SimpleClient` is:

```
%WS_SDK_HOME%\java\JAXWS\samples\com\vmware\general\SimpleClient.java
```

When you run the script, specify the Java class for the sample application along with the `--url`, `--username`, and `--password` switches on the command line. Include the complete package name in the Java class specification. The following statement shows the general format for using the `run.bat` script to run the `SimpleClient` sample application from the Java samples subdirectory for JAX-WS:

```
run.bat com.vmware.general.SimpleClient --url https://yourFQDNservername/sdk
      --username username --password password [--ignorecert ignorecert]
```

The following example shows sample output from the `SimpleClient` sample program.

Sample Output of a Successful Run of SimpleClient, Using Precompiled Java Sample

```
Object Type : Folder
Reference Value : ha-folder-vm
  Property Name : name
  Property Value : vm
Object Type : HostSystem
Reference Value : ha-host
  Property Name : name
  Property Value : sdkpubslab-02.eng.vmware.com
Object Type : ResourcePool
Reference Value : ha-root-pool
  Property Name : name
  Property Value : Resources
Object Type : Folder
Reference Value : ha-folder-host
  Property Name : name
  Property Value : host
Object Type : ComputeResource
Reference Value : ha-compute-res
  Property Name : name
  Property Value : sdkpubslab-02.eng.vmware.com
Object Type : VirtualMachine
Reference Value : 16
  Property Name : name
  Property Value : Windows_2K3_VM
...
```

```
Object Type : Datacenter
Reference Value : ha-datacenter
  Property Name : name
  Property Value : ha-datacenter
Object Type : Folder
Reference Value : ha-folder-root
  Property Name : name
  Property Value : ha-folder-root
```

To run the precompiled SimpleClient from the command prompt, do the following procedure.

Procedure

- 1 Open a Windows command prompt or shell prompt on Linux.
- 2 Navigate to the Java samples subdirectory.

```
cd %WS_SDK_HOME%\java\JAXWS\samples
```

- 3 Invoke the Java runtime, providing the full package name of the SimpleClient, server URN, credentials, and Java keyStore location, or the `--ignorecert` argument. The complete syntax is as follows:

```
java -Djavax.net.ssl.trustStore=keystore-path-or-%KEYSTORE%-environment-variable
    package-hierarchy-classname --url server-url --username username
    --password password [--ignorecert ignorecert]
```

For example:

```
java -Djavax.net.ssl.trustStore=%VMKEYSTORE% com.vmware.general.SimpleClient
    --url https://example.com/sdk --username pubs --password ***
    --ignorecert ignorecert
```

Note If error messages occur due to system heap or other memory problems, you can give the Java VM more memory, as follows:

```
java -Djavax.net.ssl.trustStore=%VMKEYSTORE% -Xms512M -Xmx1024M
    com.vmware.general.SimpleClient https://sdkpubslab-02.eng.vmware.com/sdk
    --username username
    --password password --ignorecert ignorecert
```

vSphere Server Certificates

3

The VMware vSphere API is available as a secure Web service. Secure Web service means that, by default, ESXi and vCenter Server are configured for HTTPS and support SSL to encrypt communications. This appendix explains how to manage the certificates needed for secure communications.

Read the following topics next:

- [Secure Client-Server Communications](#)
- [Simplified Security Setup for Development Environment](#)
- [Obtaining Server Certificates](#)

Secure Client-Server Communications

To connect to the server using HTTPS, client applications must verify the identity of the server by using the server's certificate during an initial handshake. The client must obtain the server certificate in advance, so that it is available during the handshake.

See [Obtaining Server Certificates](#).

Simplified Security Setup for Development Environment

You can bypass certificate checking while developing software in a non-production environment. To do this, create a custom implementation of the `javax.net.ssl.TrustManager` interface that returns `true` rather than actually verifying certificates during the SSL handshake. You can see examples of such a class in the Java code samples included with the vSphere Web Services SDK.

The Java samples included with the SDK use this technique by accepting an optional command-line argument, `--ignorecert`. If you plan to use the `--ignorecert` option or use this automatic server-certificate verification technique in your own code, you do not need to import certificates. See [Set Up for Java Development for the Web Services SDK](#) for more information.

Use the `--ignorecert` option only for development and testing purposes. Do not use it outside a firewall. If the server-certificate is not verified during the SSL handshake, the client application is subject to man-in-the-middle attacks.

Obtaining Server Certificates

VMware products use standard X.509 version 3 (X.509v3) certificates to encrypt session information sent over SSL connections between server and client systems. When a client application initiates an SSL session with the server, the server sends its certificate to the client application, which checks the X.509 certificate against a list of known Certificate Authorities (CAs) to verify the authenticity of the certificate. The client then uses the server's public key contained in the X.509 certificate to generate a random symmetric key, which it uses to encrypt all subsequent communications.

The installers for ESXi and vCenter Server create server certificates during the process of installation. For ESXi systems, the certificate name matches the DNS name of the server. For vCenter Server systems, the certificate name is VMware. Because these certificates are not signed by an official root CA, you must obtain the server certificate from each server that you plan to target with your client application and store it locally.

For example, if you are creating a client application to run against the vCenter Server and an ESXi system in standalone mode, you must obtain both the vCenter Server certificate and the ESXi certificate. If your application is aimed solely at the vCenter Server that might manage any number of ESXi systems, you must obtain the certificate only from the vCenter Server.

You can obtain the certificates in one of the following ways:

- Developers working on the Microsoft Windows platform can use the certificate-handling capabilities of the vSphere Client from the development workstation to connect to each ESXi or vCenter Server and accept the certificate into the local cache and export the certificate. See [Obtain Certificates Using the vSphere Client](#).
- Developers with access privileges on the target server systems can use a secure shell client utility (SCP, WinSCP, or SSH) to connect directly to the ESXi or vCenter Server and copy the certificates directly from the server to the development platform.

Obtain Certificates Using the vSphere Client

Use the vSphere Client to obtain certificates, so you don't have to install another client on your development workstation. You can download the VMware Certificate Authority root and leaf certificates and then add them to the operating system root store of the system from which you are connecting to the vCenter Server system.

Procedure

- 1 From a client system Web browser, go to the URL of the vCenter Server instance.
`https://my-vc-name.example.com`
- 2 Click the **Download trusted root CA certificates** link at the bottom of the grey box on the right and download the file.
- 3 If needed, change the extension of the file to `.zip`.

- 4 The file is a ZIP file of all root certificates and all CRLs in the VMware Endpoint Certificate Store (VECS).
- 5 Extract the contents of the ZIP file.
- 6 The result is a `.certs` folder that contains two types of files. Files with a number as the extension (`.0`, `.1`, and so on) are root certificates. Files with an extension that starts with an `r` (`.r0`, `.r1`, and so on) are CRL files associated with a certificate.
- 7 Install the certificate files as trusted certificates by following the process that is appropriate for your operating system.

Firefox has its own trusted roots store and does not use the operating system store. If you are working with Firefox, download the certificate as described above, and then select **Tools** > **Options**, click **Advanced**, and click **Certificates** to import the certificate into Firefox.

What to do next

After you obtain the certificate from each target server, follow the other setup steps appropriate for your programming language. For Java developers, see [Set Up for Java Development for the Web Services SDK](#).

For the latest information about certificates, see the *vSphere Security* guide at <http://docs.vmware.com/>.

Updating the Active Directory Group Policy to Accept Certificates

In some configurations, you might need to import certificates into your Active Directory domain.

If you have a configuration where the VMware Certificate Authority is an intermediate Certificate Authority, a Custom Certificate, or another certificate that is not trusted in your environment, and:

- you have a Web browser that uses the operating certificate store on Windows (such as Internet Explorer and Google Chrome)
- you can access the vCenter Server from several different machines

you can import the root certificate into the group policy of your Active Directory environment to make the certificates trusted in your Active Directory domain.

Procedure

- 1 Go to the URL of the vCenter Server system or the vCenter Server Virtual Appliance using a client system web browser.
- 2 Click the **Download trusted root CA certificates** link at the bottom of the grey box on the right and download the file.
- 3 Change the extension of the file to `.zip`.
- 4 The file is a ZIP file of all root certificates and all CRLs in the VMware Endpoint Certificate Store (VECS)

- 5 Extract the ZIP file.
- 6 The result is a `.certs` folder that contains two types of files. Files with a number extension (.0, .1, and so on) are root certificates. Files with an extension that starts with an r (.r0, r1, and so on) are CRL files associated with a certificate.
- 7 Open the **Active Directory Group Policy Management Editor**.
- 8 Open **Public Key Policies** and select **Intermediate Certification Authorities**.
- 9 Add the certificate file or files that you downloaded.
- 10 From your Windows command prompt, run `gpupdate /force` to force an update.

Firefox has its own trusted roots store and does not use the operating system store. If you are working with Firefox, download the certificate as described above, and then select **Tools** > **Options**, click **Advanced**, and click **Certificates** to import the certificate into Firefox.

Endpoint Configuration for HTTP

4

For development environments, you can simplify the connection process by configuring an HTTP connection rather than an HTTPS connection to the Web service. If your client also connects to a vSphere Automation API endpoint, you can use a similar procedure to configure the vSphere Automation API connection.

The procedure to modify the service configuration differs, depending on the service type. Choose one of the following options that applies to your situation:

- [HTTP Configuration for Web Services API Endpoint](#)
- [HTTP Configuration for vSphere Automation API Endpoint](#)

Read the following topics next:

- [Modifying Service Endpoint Configurations to Support HTTP](#)
- [HTTP Configuration for Web Services API Endpoint](#)
- [HTTP Configuration for vSphere Automation API Endpoint](#)

Modifying Service Endpoint Configurations to Support HTTP

ESXi, vCenter Server, and vSphere Automation API endpoints run by default on port 443, as secure Web services that can be accessed using SSL or TLS over HTTP (HTTPS). However, for a development environment, you might want to simplify the connection process from a client application by configuring the target services to support HTTP.

Note The HTTP protocol without SSL or TLS is insecure. Your user credentials could be intercepted by wire capture software.

The API service endpoints are handled by a reverse-proxy service, which has a configuration file that can be modified to specify support for HTTP as an accepted protocol. If you configure the service for HTTP, you do not need to import the server certificates on the client development workstation. Modifying the service configuration to support HTTP access is recommended for test or development environments only, not for production deployments. The default protocol, HTTPS, provides better security for production deployments.

HTTP Configuration for Web Services API Endpoint

You can modify the Web Services API endpoint configuration to accept HTTP connections, in addition to or instead of HTTPS connections.

HTTP Configuration for Web Services API Endpoint on ESXi or vCenter Server for Windows

This procedure applies to version 5.5 or later ESXi or vCenter Server for Windows.

You can modify ESXi configuration from a shell window over an SSH connection, using the following procedure. If you do not have SSH enabled, use the appropriate vSphere CLI command to obtain the configuration file from the server, modify the file to support HTTP, and move the file back to the ESXi system. For more information about the vSphere CLI command syntax, see the *vSphere CLI Installation and Reference Guide*.

Procedure

- 1 Log in to a shell window or File Explorer with **root** or **administrator** privileges.
- 2 Change directories to the location of the endpoint configuration file.

The location differs, depending on the platform.

- For ESXi:

```
/etc/vmware/rhttpproxy
```

- For vCenter Server for Windows:

```
C:\Program Data\VMware\vCenterServer\cfg\vmware-  
rhttpproxy\endpoints.conf.d
```

- 3 Copy the `endpoints.conf` file to a temporary directory for editing.

- On ESXi:

```
# cp endpoints.conf /tmp/endpoints.conf
```

- On vCenter Server for Windows, use File Explorer to copy the file.

- 4 Change the permissions on the temporary `endpoints.conf` file to allow editing.

- On ESXi:

```
# chmod +w /tmp/endpoints.conf
```

- On vCenter Server for Windows, right click the file in File Explorer and select **Properties** to change file permissions.

- 5 Use a text editor to open the temporary file.

- On ESXi:

```
# vi /tmp/endpoints.conf
```

- On vCenter Server for Windows, choose any text editor, such as Notepad, from the **Start** menu.

- 6 Navigate to the line that specifies the endpoints for SDK connections, which begins with /sdk.

The line looks similar to this:

```
/sdk    local    8085                redirect    allow
```

- 7 To enable HTTP connections, change the word `redirect` to `allow`.

When configured to allow both HTTP and HTTPS connections, the /sdk line looks similar to this:

```
/sdk    local    8085                allow      allow
```

- 8 (Optional) If you prefer to completely disable HTTPS, change the last word to `reject` instead of `allow`.

When configured to allow only HTTP connections, the /sdk line looks similar to this:

```
/sdk    local    8085                allow      reject
```

- 9 (Optional) Change the setting for the Managed Object Browser as well.

When configured to allow both HTTP and HTTPS connections, the /mob line looks similar to this:

```
/mob    local    8085                allow      allow
```

- 10 Save your settings and close the file.

- 11 Change the permissions on the temporary file to disable editing.

- On ESXi:


```
# chmod -w /tmp/endpoints.conf
```
- On vCenter Server for Windows, right click the file in File Explorer and select **Properties** to change file permissions.

- 12 Copy the original `endpoints.conf` file to a backup file.

- On ESXi:


```
# cp endpoints.conf endpoints.conf.old
```
- On vCenter Server for Windows, use File Explorer to copy the file.

- 13 Copy the temporary file `endpoints.conf` file back, replacing the original `endpoints.conf` file.

- On ESXi:


```
# cp /tmp/endpoints.conf endpoints.conf
```
- On vCenter Server for Windows, use File Explorer to copy the file.

- 14 Signal the reverse proxy service to update its configuration by entering the following command:

- On ESXi:

```
/etc/init.d/rhttpproxy restart
```

- On vCenter Server for Windows:

From the Windows menu, choose **Control Panel > Administrative Tools > Services**, right click the rhttpproxy service, and choose **Restart**.

Example: An `endpoints.conf` File Modified To Support HTTP connections to the SDK and the MOB

```

/                local            8309            redirect        allow
/sdk             local            8307            allow           allow
/client/clients.xml local        8309            allow           allow
/ui             local            8308            redirect        allow
/vpxa          local            8089            reject          allow
/mob           namedpipe        /var/run/vmware/proxy-mob allow           allow
/wsman        local            8889            redirect        allow
/sdkTunnel    namedpipetunnel /var/run/vmware/proxy-sdk-tunnel allow           reject
/ha-nfc       local            12001           allow           allow
/nfc          local            12000           allow           allow
/folder       local            8309            redirect        allow
/host         local            8309            redirect        allow
/tmp          local            8309            redirect        allow
/screen       local            8309            redirect        allow
/guestFile    local            8309            redirect        allow
/cgi-bin      local            8309            redirect        allow

```

HTTP Configuration for Web Services API Endpoint on vCenter Server Appliance

You can modify the Web proxy service to support HTTP on vCenter Server Appliance.

You can modify from a shell window over an SSH connection, using the following procedure. If you do not have SSH enabled, see *vCenter Server Appliance Configuration* or *VMware vCenter Server Appliance Programming Guide*. This procedure applies to version 6.0 or later vCenter Server Appliance.

Procedure

- 1 Log in to a shell window with `root` privileges.
- 2 Change directories to the location of the endpoint configuration file.
 - For vCenter Server Appliance:

```
cd /etc/vmware-rhttpproxy/endpoints.conf.d
```
- 3 Copy the `endpoints.conf` file to a temporary directory for editing.
 - On vCenter Server Appliance:

```
# cp vpxd-rhttpproxy-endpoint.conf /tmp/vpxd-rhttpproxy-endpoint.conf
```

- 4 Change the permissions on the temporary `vpxd-rhttpproxy-endpoint.conf` file to allow editing.

- On vCenter Server Appliance:
chmod +w /tmp/vpxd-rhttpproxy-endpoint.conf

- 5 Use a text editor to open the temporary file.

- On vCenter Server Appliance:
vi /tmp/vpxd-rhttpproxy-endpoint.conf

- 6 Navigate to the line that specifies the endpoints for SDK connections, which begins with `/sdk`.

The line looks similar to this:

```
/sdk    local    8085                redirect    allow
```

- 7 To enable HTTP connections, change the word `redirect` to `allow`.

When configured to allow both HTTP and HTTPS connections, the `/sdk` line looks similar to this:

```
/sdk    local    8085                allow      allow
```

- 8 (Optional) If you prefer to completely disable HTTPS, change the last word to `reject` instead of `allow`.

When configured to allow only HTTP connections, the `/sdk` line looks similar to this:

```
/sdk    local    8085                allow      reject
```

- 9 (Optional) Change the setting for the Managed Object Browser as well.

When configured to allow both HTTP and HTTPS connections, the `/mob` line looks similar to this:

```
/mob    local    8085                allow      allow
```

- 10 Save your settings and close the file.

- 11 Change the permissions on the temporary file to disable editing.

- On vCenter Server Appliance:
chmod -w /tmp/vpxd-rhttpproxy-endpoint.conf

- 12 Copy the original `endpoints.conf` file to a backup file.

- On vCenter Server Appliance:
cp vpxd-rhttpproxy-endpoint.conf vpxd-rhttpproxy-endpoint.conf.old

- 13 Copy the temporary file `endpoints.conf` file back, replacing the original `endpoints.conf` file.

- On vCenter Server Appliance:
cp /tmp/vpxd-rhttpproxy-endpoint.conf vpxd-rhttpproxy-endpoint.conf

14 Signal the reverse proxy service to update its configuration by entering the following command:

- On vCenter Server Appliance:

```
/etc/init.d/vmware-rhttpproxy restart
```

For an example of the contents of a `vpxd-rhttpproxy-endpoint.conf` file modified to support HTTP connections, see [HTTP Configuration for Web Services API Endpoint](#).

HTTP Configuration for vSphere Automation API Endpoint

You can also modify the vAPI endpoint configuration for vCenter Server to accept HTTP connections in addition to or instead of HTTPS connections. This is useful for clients that interact both with the vSphere Web Services API endpoint and the vSphere Automation API endpoint in a development environment. Use the following procedure.

Procedure

1 Log in to a shell window or File Explorer with **root** or **administrator** privileges.

2 Change directories to the location of the endpoint configuration file.

The location differs, depending on the platform.

- For vCenter Server Appliance:

```
/etc/vmware-rhttpproxy/endpoints.conf.d
```

- For vCenter Server for Windows:

```
C:\Program Data\VMware\vCenterServer\cfg\vmware-rhttpproxy\endpoints.conf.d
```

3 Copy the `vapi-endpoint.conf` file to a temporary directory for editing.

- On vCenter Server Appliance:

```
# cp vapi-endpoint.conf /tmp/vapi-endpoint.conf
```

- On vCenter Server for Windows, use File Explorer to copy the file.

4 Change the permissions on the temporary file to allow editing.

- On vCenter Server Appliance:

```
# chmod +w /tmp/vapi-endpoint.conf
```

- On vCenter Server for Windows, right click the file in File Explorer and select **Properties** to change file permissions.

5 Use a text editor to open the temporary file.

- On vCenter Server Appliance:

```
# vi /tmp/vapi-endpoint.conf
```

- On vCenter Server for Windows, choose any text editor, such as Notepad, from the **Start** menu.

- 6 Navigate to the line that specifies the endpoint for REST connections, which begins with `/rest`.

The line looks similar to this:

```
/rest    local    12346                redirect    allow
```

- 7 To enable HTTP connections for REST clients, change the word `redirect` to `allow`.

When configured to allow both HTTP and HTTPS connections, the `/rest` line looks similar to this:

```
/rest    local    12346                allow      allow
```

- 8 (Optional) If you prefer to completely disable HTTPS, change the last word to `reject` instead of `allow`.

When configured to allow only HTTP connections, the `/rest` line looks similar to this:

```
/rest    local    12346                allow      reject
```

- 9 Navigate to the line that specifies the endpoint for clients that use language bindings rather than REST, which begins with `/api`.

The line looks similar to this:

```
/api     local    12346                redirect    allow
```

- 10 To enable HTTP connections for clients using language bindings rather than REST, change the word `redirect` to `allow`.

When configured to allow both HTTP and HTTPS connections, the `/api` line looks similar to this:

```
/api     local    12346                allow      allow
```

- 11 Save your settings and close the file.

- 12 Change the permissions on the temporary file to disable editing.

- On vCenter Server Appliance:
chmod -w /tmp/vapi-endpoint.conf
- On vCenter Server for Windows, right click the file in File Explorer and select **Properties** to change file permissions.

- 13 Copy the original `vapi-endpoint.conf` file to a backup file.

- On vCenter Server Appliance:
cp vapi-endpoint.conf vapi-endpoint.conf.old
- On vCenter Server for Windows, use File Explorer to copy the file.

- 14 Copy the temporary file back, replacing the original `vapi-endpoint.conf` file.

- On vCenter Server Appliance:
cp /tmp/vapi-endpoint.conf vapi-endpoint.conf

- On vCenter Server for Windows, use File Explorer to copy the file.

15 Signal the reverse proxy service to update its configuration by entering the following command:

- On vCenter Server Appliance:
/etc/init.d/vmware-rhttpproxy restart

- On vCenter Server for Windows:

From the Windows menu, choose **Control Panel > Administrative Tools > Services**, right click the rhttpproxy service, and choose **Restart**.

Example: A `vapi-endpoint.conf` File Modified To Support HTTP connections for API and REST

```

/vapiendpoint/health      local      12346     allow     allow
/vapiendpoint/resourcebundle local      12346     allow     allow
/rest                     local      12346     allow     allow
/site/api                 local      12346     redirect  allow
/site/rest                local      12346     redirect  allow
/api/                     local      12346     allow     allow

```