

Template for Citrix XenApp Installation

Table of Contents

- Installation 2**
 - Basic Installation steps 2
 - Install the Splunk Universal Forwarder on Each XenApp Server 3**
 - Manual Installation of the Splunk Universal Forwarder 3
 - Silent Installation 8
 - Installing on a Shared Image such as Citrix Provisioning Services (PVS) or Machine Creation Services (MCS)..... 9
 - Post Installation Steps 9**
 - Set the Splunk Universal Forwarder Account..... 9*
 - Set PowerShell Execution Policy..... 9*
 - Install the Splunk Template for XenApp on your Splunk server 9**
 - Copy the appropriate Universal Forwarder configuration files to the XenApp Servers 10**
 - How the Add-ons Work..... 10
 - Using the Template for Citrix XenApp..... 11**

Overview

The Template for Citrix XenApp includes several “out-of-the-box” use cases including:

- High-level overviews supporting multiple farms
- Alerting
- ICA latency reporting
- User experience investigation
- User logon time details
- Performance visualization and monitoring
- Application usage
- Critical service monitoring

Since the overall ecosystem of XenApp environments will vary from company to company, the Template for Citrix XenApp is meant to be a starting point for using Splunk with Citrix XenApp. The template is designed in such a way as to be easily customized to fit specific needs.

Installation

There two basic steps to any Splunk application:

1. Getting data in to Splunk.
2. Analyzing/reporting on the data.

The Template for Citrix XenApp takes care of both of these steps. The first step (getting data into Splunk) involves installing a collection mechanism called a Universal Forwarder on the various XenApp servers based on server role. The second step is accomplished by installing the Template for Citrix XenApp on the Splunk server. The Template for Citrix XenApp includes several dashboards, forms, alerts, and searches pre-configured. However, you are not limited to these out-of-the-box use cases. Dashboards can be modified or created to specifically suit your needs by following the official Splunk documentation at <http://docs.splunk.com>

Basic Installation steps

- 1) Install the Splunk Server.
- 2) Install the Splunk Universal Forwarder on the XenApp Servers.
- 3) Install the Template for Citrix XenApp on the Splunk Server.
- 4) Copy the appropriate Universal Forwarder configuration files to the XenApp Servers. The following configuration files are based on the XenApp server role and include:
 - a. Zone Data Collector (ZDC)
 - b. XML Server
 - c. Application Server

Install the Splunk Server

The Splunk server components can be installed on a variety of operating systems including Microsoft Windows and Linux. The Template for Citrix XenApp is not dependent on the operating system on which the Splunk server components are installed. You may choose any platform you like.

<http://www.splunk.com/download>

The Splunk server components can be installed on a single server or a distributed environment for scalability and high availability. For more information, reference the official Splunk documentation online:

<http://docs.splunk.com/Documentation/Splunk/latest/Installation>

Install the Splunk Universal Forwarder on Each XenApp Server

The Splunk Universal Forwarder is a piece of software that gathers specified information from the various Citrix XenApp servers. By default, the Splunk Universal Forwarder does nothing if installed as specified in this manual. Later during the installation process, the data gathering configurations will be specified for each Citrix XenApp server role type - i.e. Zone Data Collectors, XML Servers, and Application Servers.

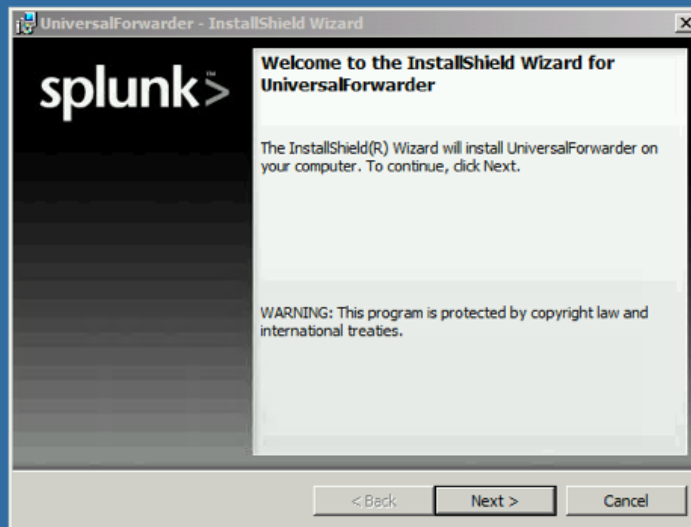
Download the Splunk Universal Forwarder for Windows from the following location:

<http://www.splunk.com/download/universalforwarder>

Manual Installation of the Splunk Universal Forwarder

This needs to be completed on each XenApp server regardless of role. Silent installation instructions are available in this manual as well.

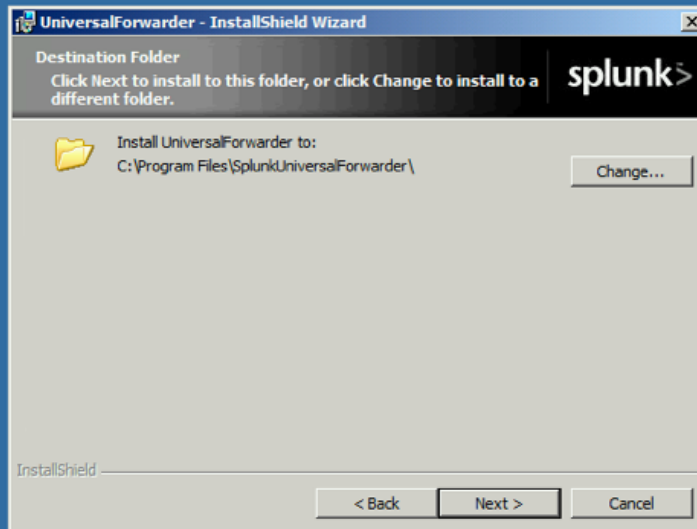
1. Start the installation by double clicking the downloaded file from above.



2. Accept the License Agreement.

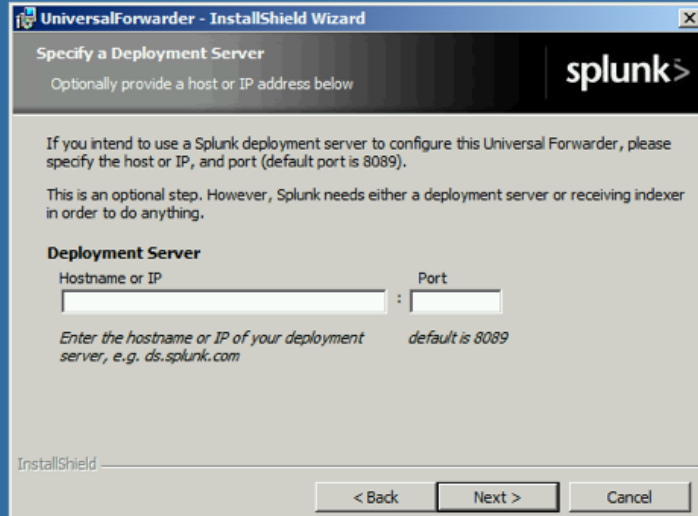


3. Choose and installation folder.

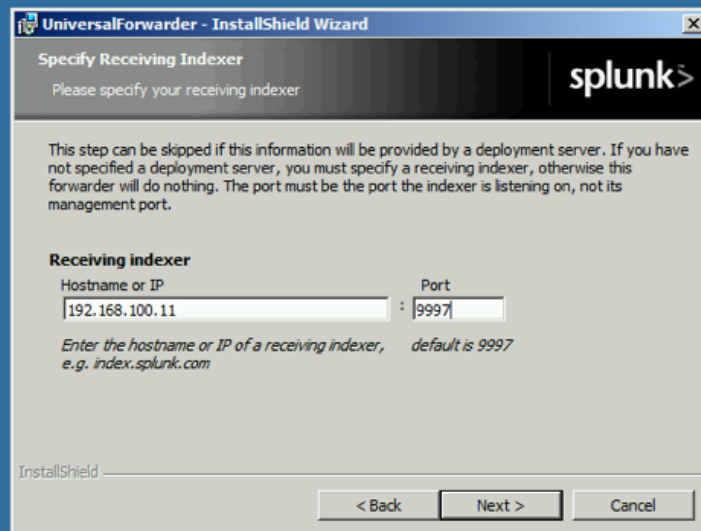


4. Leave the Deployment Server settings empty for simple installations. For more information about centralizing configurations, read about Deployment Server here ->

<http://docs.splunk.com/Documentation/Splunk/latest/UPdating/Aboutdeploymentserver>



5. Enter the IP address or FQDN and listening port of your Splunk server.
By default, the listening port on the Splunk server is 9997.



The screenshot shows the 'Specify Receiving Indexer' step of the UniversalForwarder - InstallShield Wizard. The window title is 'UniversalForwarder - InstallShield Wizard' and the Splunk logo is in the top right. The main heading is 'Specify Receiving Indexer' with the instruction 'Please specify your receiving indexer'. A note states: 'This step can be skipped if this information will be provided by a deployment server. If you have not specified a deployment server, you must specify a receiving indexer, otherwise this forwarder will do nothing. The port must be the port the indexer is listening on, not its management port.' Below this, the 'Receiving indexer' section has two input fields: 'Hostname or IP' with the value '192.168.100.11' and 'Port' with the value '9997'. A hint text says: 'Enter the hostname or IP of a receiving indexer, default is 9997 e.g. index.splunk.com'. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

6. Leave the SSL certificate information empty for simple installations.

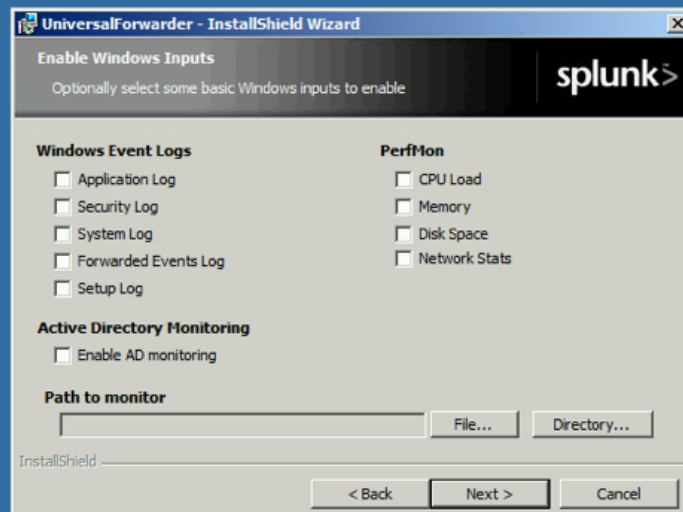


The screenshot shows the 'Certificate Information' step of the UniversalForwarder - InstallShield Wizard. The window title is 'UniversalForwarder - InstallShield Wizard' and the Splunk logo is in the top right. The main heading is 'Certificate Information' with the instruction 'Optionally provide certificate information for verifying the identity of this machine'. A note states: 'If the following certificate information is not provided, forwarded data will still be encrypted with the default Splunk certificate.' Below this, there are three sections: 1. 'SSL Certificate (file containing public and private key pair)' with a text box and a 'Browse...' button. 2. 'Certificate Password' with 'Enter password' and 'Confirm password' labels and corresponding text boxes. 3. 'SSL Root CA (file containing the Root CA certificate to validate the server certificate)' with a text box and a 'Browse...' button. At the bottom are buttons for '< Back', 'Next >', and 'Cancel'.

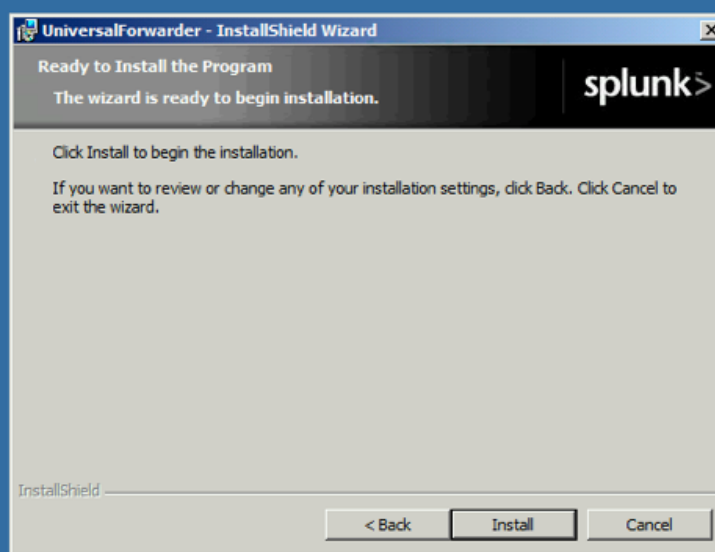
7. Select the option to collect Local Data Only.



8. Leave all options **unchecked**. The configuration file that will be added later will tell the Universal Forwarder what to collect. If you select options here, duplicate data may be collected and inflate your daily indexing volume.



9. Click the Install button to finish the installation.



10. Click the Finish button.



Silent Installation

The Splunk Universal Forwarder can be installed on the command line silently. This is convenient for installing the Universal Forwarder via traditional software delivery mechanisms. Here is an example (be sure to change the IP address for your RECEIVING_INDEXER and to substitute the asterisk "*" for the version of the Splunk Universal Forwarder version you downloaded):

```
msiexec /i splunkforwarder*.msi AGREETOLICENSE=yes  
RECEIVING_INDEXER=192.168.100.11:9997 /quiet
```


Installing on a Shared Image such as Citrix Provisioning Services (PVS) or Machine Creation Services (MCS)

The Splunk Universal Forwarder can be installed on a shared system image such as Citrix Provisioning Services (PVS) or Machine Creations Services (MSC). Follow the instructions outlined in the Splunk documentation found here:

<http://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Makeadfpartofasystemimage>

Post Installation Steps

Set the Splunk Universal Forwarder Account

The Splunk Universal Forwarder needs to be run as a local administrator as well as a XenApp farm administrator.

Start the Windows Services console and change the “Log On As” account for the “SplunkForwarder” service.

Set PowerShell Execution Policy

The Splunk Universal Forwarder utilizes Microsoft PowerShell to gather Citrix-specific information. Therefore, the Microsoft PowerShell Execution Policy needs to be set as RemoteSigned. To do this, launch PowerShell on your XenApp server and execute the following command:

```
Set-ExecutionPolicy RemoteSigned
```

A Group Policy Object (GPO) can also be used to set the PowerShell Execution Policy.

```
Computer Configuration | Administrative Templates | Windows Components | Windows PowerShell >> configure the Turn On Script Execution setting
```

Install the Splunk Template for XenApp on your Splunk server

Download and unzip the Template for Citrix XenApp from <http://apps.splunk.com>

Copy the TemplateForXenApp folder to the Splunk server in the following location:

```
$SPLUNK_HOME\etc\apps
```

By default, \$SPLUNK_HOME is:

```
C:\Program Files\Splunk for Windows  
/opt/splunk for *nix
```

Restart Splunk by executing the following command:

```
C:\Program Files\Splunk\bin\splunk.exe restart
```

Copy the appropriate Universal Forwarder configuration files to the XenApp Servers

By default, the Splunk Universal Forwarders installed on the XenApp servers earlier do not do anything. A Universal Forwarder configuration (called an add-on) needs to be copied to the appropriate XenApp servers based on role. The Splunk Universal Forwarder configurations can be found in the following location on your Splunk server:

```
$SPLUNK_HOME\etc\apps\TemplateForXenApp\appserver\addons
```

There are 3 add-ons to distribute to the XenApp servers.

1. TA-XA6x-Server goes on all XenApp servers that host user sessions.
2. TA-XA6x-ZDC goes on all dedicated Zone Data Collectors
3. TA-XA6x-XML goes on all servers designated as Citrix XML servers.

How the Add-ons Work

These add-ons “tell” the Splunk Universal Forwarder what types of information to collect and forwards the results to the Splunk server for indexing/analysis. The information gathered is completely configurable. The add-ons use 3 primary methods of gathering data:

1. inputs.conf – this is the heart of the collection mechanism. inputs.conf is a text file that has several configuration options. All the options for inputs.conf can be found here:
<http://docs.splunk.com/Documentation/Splunk/latest/admin/inputsconf>
2. wmi.conf – this file is similar to inputs.conf and is used primarily for gathering WMI data. All the options for wmi.conf can be found here:
<http://docs.splunk.com/Documentation/Splunk/latest/admin/wmiconf>
3. Scripted Inputs – scripted inputs can be any script that the operating system understands. For Microsoft Windows, this could be a .bat file, a .cmd file, an operating system command like quser, PowerShell script, etc. Anything that gets written to stdout (the screen by default) will end up in the Splunk index. This makes it very easy to create and test your own scripts to gather data and extend Splunk.

All of the collection mechanisms are completely configurable. You are free to change intervals, remove collection metrics, add your own collection metrics, modify or create scripts, etc.

Using the Template for Citrix XenApp

More documentation about using the Template for Citrix XenApp can be found by navigating to your Splunk instance where you installed the Template for Citrix XenApp and clicking the “Help” menu option. For example:

http://localhost:8000/en-US/app/TemplateForXenApp/help_using