Template for Citrix XenDesktop 7 Installation

Table of Contents

Overview

The Template for Citrix XenDesktop 7 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 XenDesktop environments will vary from company to company, the Template for Citrix XenDesktop 7 is meant to be a starting point for using Splunk with Citrix XenDesktop. 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 XenDesktop 7 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 XenDesktop machines based on machine role. The second step is accomplished by installing the Template for Citrix XenDesktop 7 on the Splunk server. The Template for Citrix XenDesktop 7 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 XenDesktop Machines.
3) Install the Template for Citrix XenDesktop 7 on the Splunk Server.
4) Copy the appropriate Universal Forwarder configuration files to the XenDesktop Machines. The following configuration files are based on the XenDesktop machine role and include:
    a. Desktop Broker.
    b. Desktop or Server with the Citrix Virtual Delivery Agent (VDA) installed.

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 XenDesktop 7 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

Enable Receiving on the Splunk Server

After installing the Splunk server, enable the server to receive data from the deployed Universal Forwarders (details below). Detailed directions on setting up receiving can be found at the following location:
http://docs.splunk.com/Documentation/Splunk/latest/Forwarding/Enableareceiver

Create Indexes on the Splunk Indexing Tier

The XenDesktop Universal Forwarder configurations are pre-configured to send data to specific event indexes. These event indexes need to be created on the Splunk indexing tier. Detailed directions for creating event indexes can be found at the following location:
https://docs.splunk.com/Documentation/Splunk/latest/Indexer/Setupmultipleindexes

Create event indexes with the following names:

- xd
- xd_perfmon
- xd_winevents
- xd_alerts

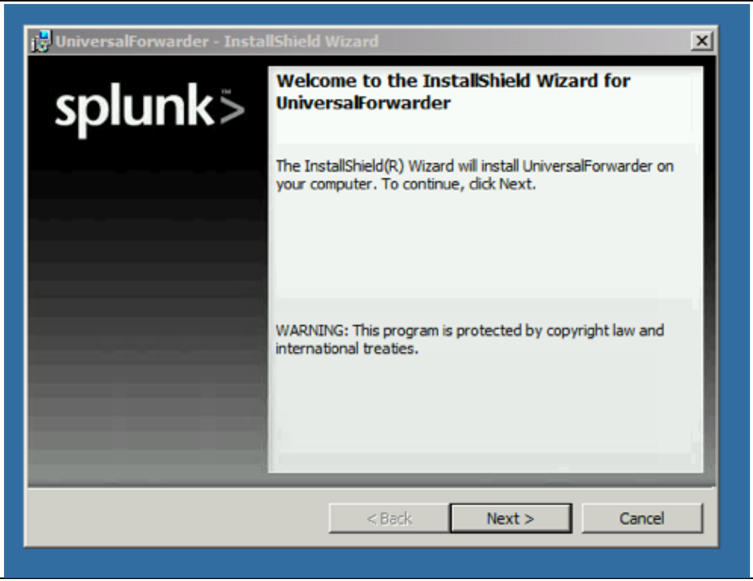
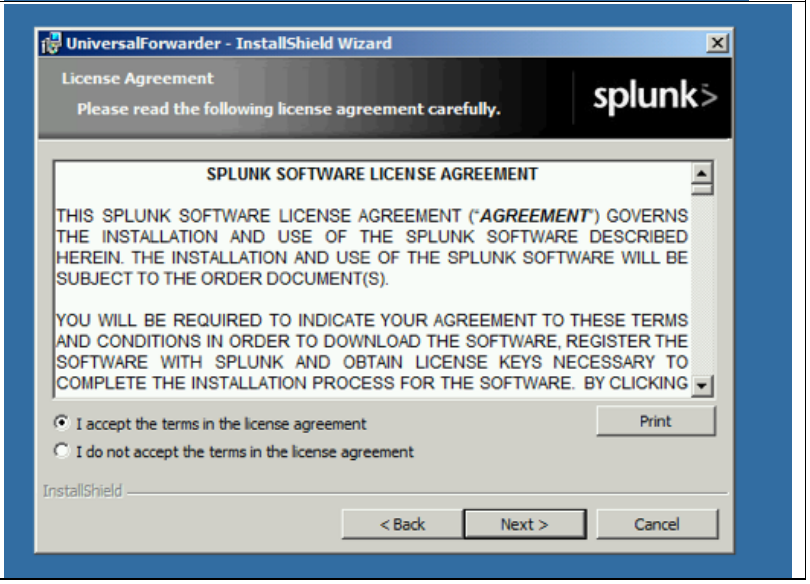
Install the Splunk Universal Forwarder on Each XenDesktop Machine

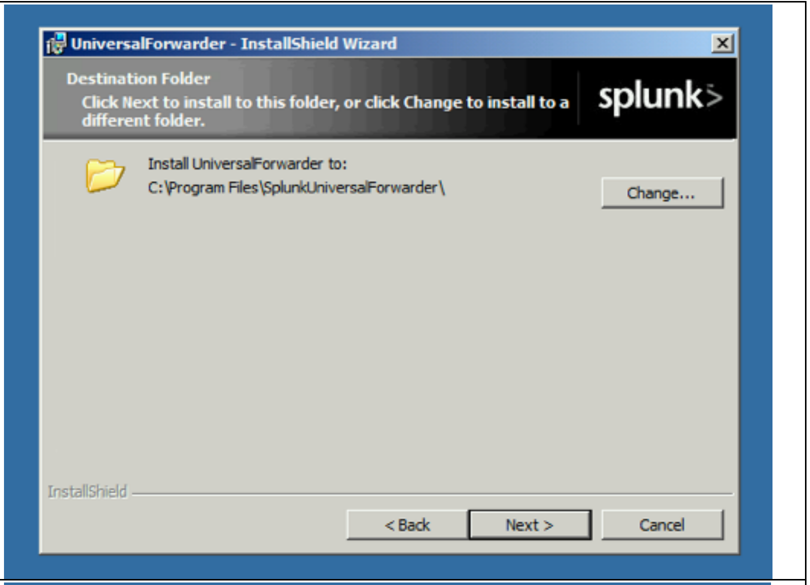
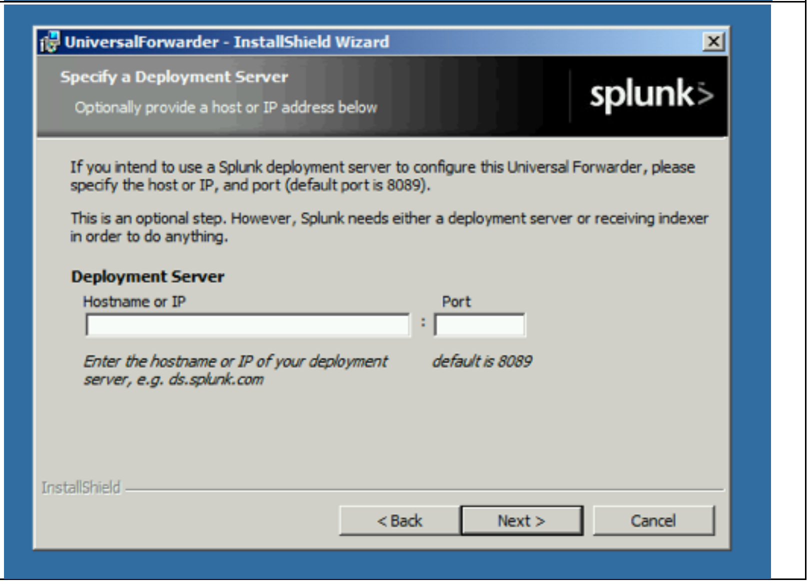
The Splunk Universal Forwarder is a piece of software that gathers specified information from the various Citrix XenDesktop machines. By default, the Splunk Universal Forwarder does nothing if installed as specified in this manual. Later during the installation process, the data gathering configurations will be specified for each Citrix XenDesktop machine role type - i.e. Desktop Broker and VDA.

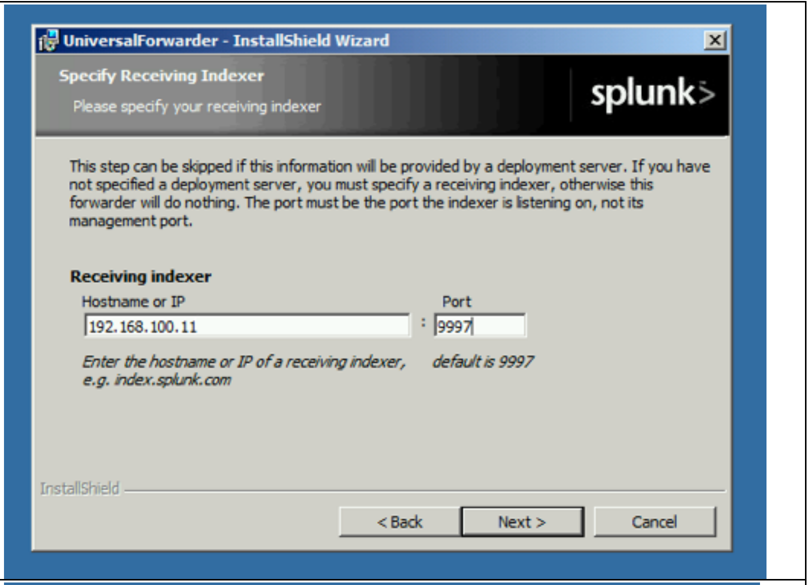
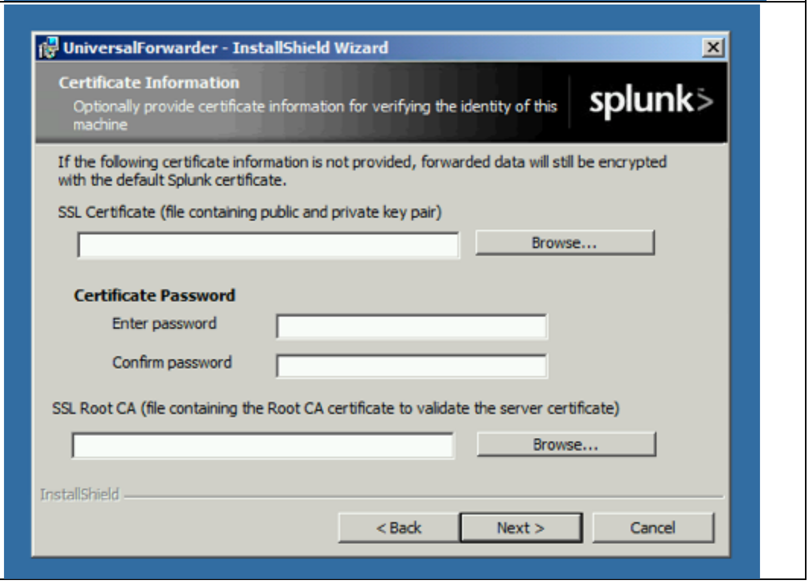
Download the Splunk Universal Forwarder for Windows from the following location:
http://www.splunk.com/download/universalforwarder

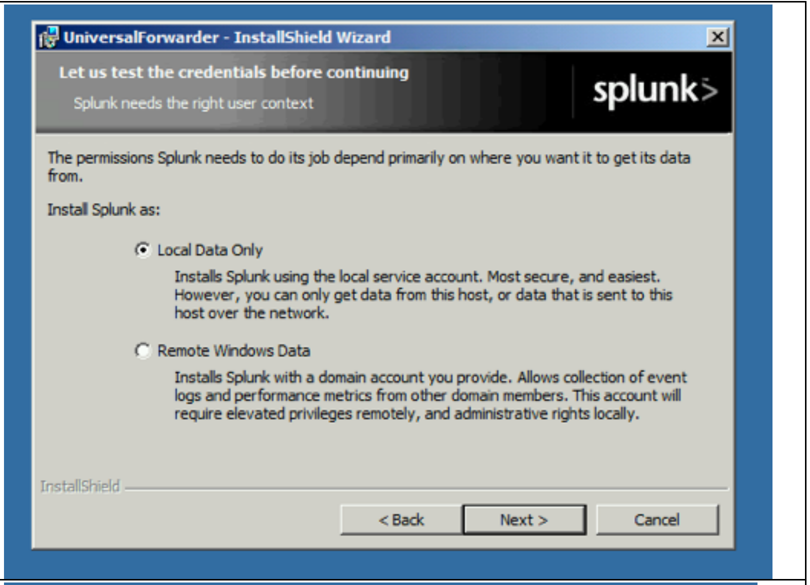
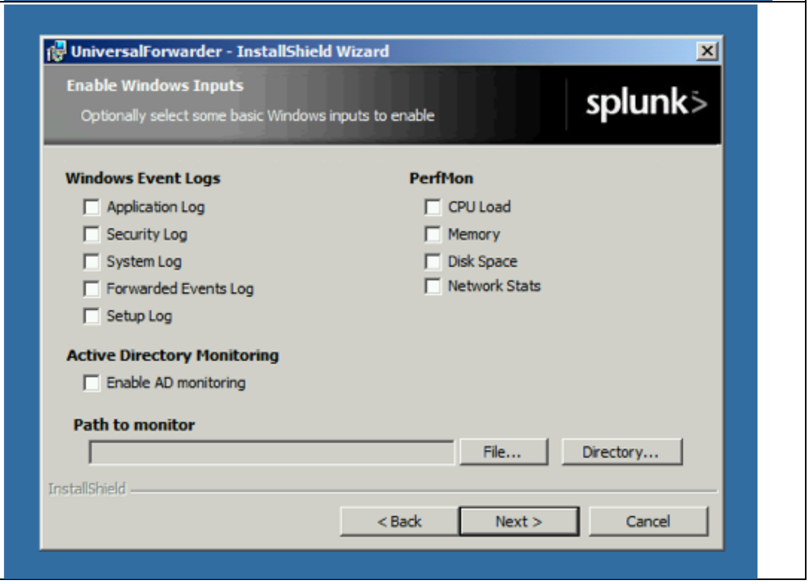
Manual Installation of the Splunk Universal Forwarder

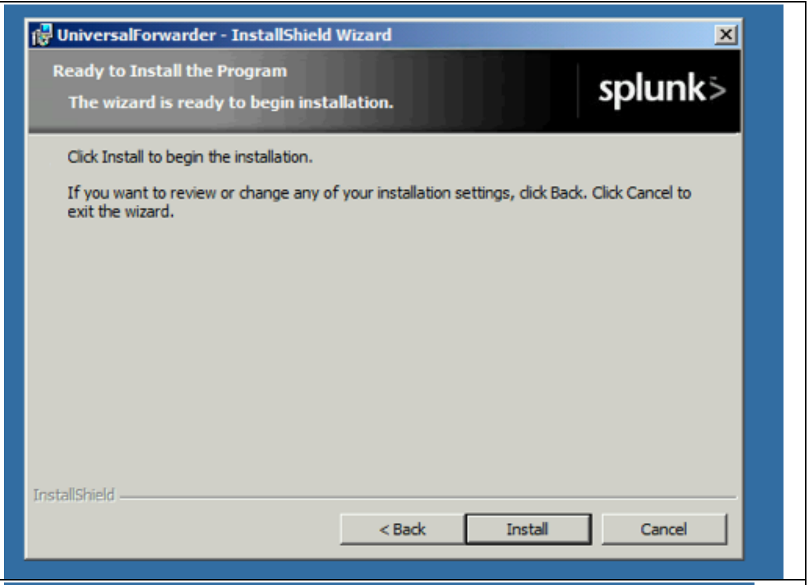
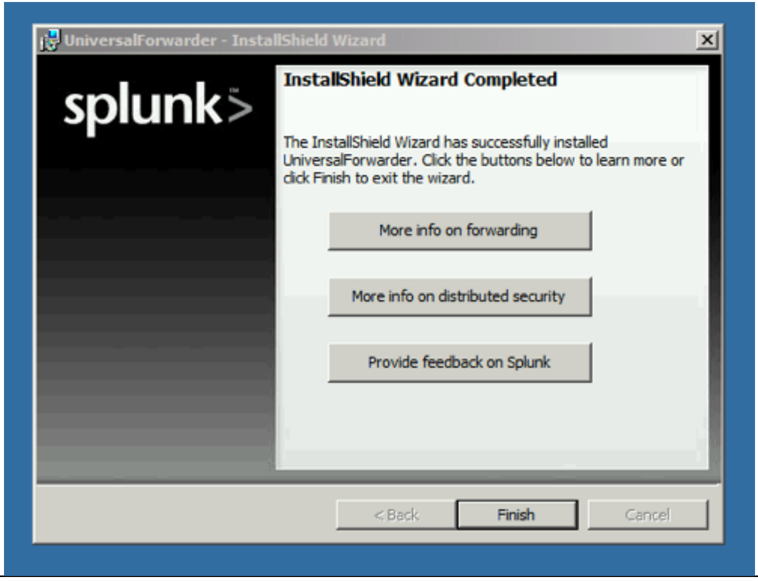
This needs to be completed on each XenDesktop machine regardless of role. Silent installation instructions are available in this manual as well.

1. Start the installation by double clicking the downloaded file from above.	 UniversalForwarder - InstallShield Wizard **Welcome to the InstallShield Wizard for UniversalForwarder** The InstallShield(R) Wizard will install UniversalForwarder on your computer. To continue, click Next. WARNING: This program is protected by copyright law and international treaties.
2. Accept the License Agreement.	 UniversalForwarder - InstallShield Wizard License Agreement Please read the following license agreement carefully. SPLUNK SOFTWARE LICENSE AGREEMENT THIS SPLUNK SOFTWARE LICENSE AGREEMENT ("*AGREEMENT*") GOVERNS THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE DESCRIBED HEREIN. THE INSTALLATION AND USE OF THE SPLUNK SOFTWARE WILL BE SUBJECT TO THE ORDER DOCUMENT(S). YOU WILL BE REQUIRED TO INDICATE YOUR AGREEMENT TO THESE TERMS AND CONDITIONS IN ORDER TO DOWNLOAD THE SOFTWARE, REGISTER THE SOFTWARE WITH SPLUNK AND OBTAIN LICENSE KEYS NECESSARY TO COMPLETE THE INSTALLATION PROCESS FOR THE SOFTWARE. BY CLICKING ● I accept the terms in the license agreement ○ I do not accept the terms in the license agreement splunk> Print InstallShield < Back Next > Cancel

3. Choose and installation folder.	 UniversalForwarder - InstallShield Wizard Destination Folder Click Next to install to this folder, or click Change to install to a different folder. Install UniversalForwarder to: C:\Program Files\SplunkUniversalForwarder\\ splunk> Change... InstallShield < Back Next > Cancel
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	 UniversalForwarder - InstallShield Wizard Specify a Deployment Server Optionally provide a host or IP address below If you intend to use a Splunk deployment server to configure this Universal Forwarder, please specify the host or IP, and port (default port is 8089). This is an optional step. However, Splunk needs either a deployment server or receiving indexer in order to do anything. **Deployment Server** Hostname or IP: Port: *Enter the hostname or IP of your deployment server, e.g. ds.splunk.com* *default is 8089*

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.	 UniversalForwarder - InstallShield Wizard splunk> InstallShield < Back Next > Cancel **Specify Receiving Indexer** Please specify your receiving indexer 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. **Receiving indexer** Hostname or IP: 192.168.100.11 Port: 9997 *Enter the hostname or IP of a receiving indexer, e.g. index.splunk.com* *default is 9997*
6. Leave the SSL certificate information empty for simple installations.	 UniversalForwarder - InstallShield Wizard splunk> Browse... Browse... InstallShield < Back Next > Cancel **Certificate Information** Optionally provide certificate information for verifying the identity of this machine If the following certificate information is not provided, forwarded data will still be encrypted with the default Splunk certificate. SSL Certificate (file containing public and private key pair) **Certificate Password** Enter password Confirm password SSL Root CA (file containing the Root CA certificate to validate the server certificate)

7. Select the option to collect Local Data Only.	 UniversalForwarder - InstallShield Wizard **Let us test the credentials before continuing** Splunk needs the right user context The permissions Splunk needs to do its job depend primarily on where you want it to get its data from. Install Splunk as: ● Local Data Only Installs Splunk using the local service account. Most secure, and easiest. However, you can only get data from this host, or data that is sent to this host over the network. ○ Remote Windows Data Installs Splunk with a domain account you provide. Allows collection of event logs and performance metrics from other domain members. This account will require elevated privileges remotely, and administrative rights locally. InstallShield < Back · Next > · Cancel
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.	 UniversalForwarder - InstallShield Wizard **Enable Windows Inputs** Optionally select some basic Windows inputs to enable **Windows Event Logs** ☐ Application Log ☐ Security Log ☐ System Log ☐ Forwarded Events Log ☐ Setup Log **PerfMon** ☐ CPU Load ☐ Memory ☐ Disk Space ☐ Network Stats **Active Directory Monitoring** ☐ Enable AD monitoring **Path to monitor** File... · Directory... InstallShield < Back · Next > · Cancel

9. Click the Install button to finish the installation.	 UniversalForwarder - InstallShield Wizard Ready to Install the Program The wizard is ready to begin installation. Click Install to begin the installation. If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.
10. Click the Finish button.	 UniversalForwarder - InstallShield Wizard InstallShield Wizard Completed The InstallShield Wizard has successfully installed UniversalForwarder. Click the buttons below to learn more or click Finish to exit the wizard. splunk> More info on forwarding More info on distributed security Provide feedback on Splunk < Back Finish Cancel

Silent Installation

The Splunk Universal Forwarder can be installed on the command line silently. This is convenient for installing the Universal Forward 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. On Desktop Broker machines, the Splunk Universal Forwarder needs to run as a XenDesktop site administrator so that the PowerShell scripts will have access to the XenDesktop site information.

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 XenDesktop machines 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 XenDesktop on your Splunk server

Download and unzip the Template for Citrix XenDesktop 7 from http://apps.splunk.com

Copy the TemplateForXenDesktop 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 XenDesktop Machines

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

https://github.com/splunk/splunk-template-xendesktop-7/tree/master/add-ons

There are 2 add-ons to distribute to the XenDesktop machines.

1. TA-XD7-Broker goes on all XenDesktop Brokers.
2. TA-XD7-VDA goes on all desktops or servers that have the Citrix Virtual Delivery Agent (VDA) installed.

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 XenDesktop 7

More documentation about using the Template for Citrix XenDesktop 7 can be found by navigating to your Splunk instance where you installed the Template for Citrix XenDesktop 7 and clicking the "Help" menu option. For example: http://localhost:8000/en-US/app/TemplateForXenDesktop/help_using