# Setting up Monitoring for Xendesktop and Citrix PVS probes.

This document is a higher level guideline and contains data from the Citrix Xendesktop guide. The idea for this document is to show some examples and help you to prepare for successfully and painlessly configuring monitoring for Citrix Xendesktop and Citrix PVS probes.

Monitoring of a Citrix Xendesktop environment is going to take some planning in order to make sure your have all of the proper configuration settings in order for the probe to connect properly to the Xendesktop environment. The major areas to be aware of is to validate that the Powershell and WinRM setting are correctly configured on the (DCC) Server, also known as the Xendesktop Delivery Controller Server.

## **Prerequisites or DCC Controller Settings**

This section describes the prerequisites for this probe:

* XenDesktop version 5.5 or later environment.
* Windows PowerShell command line interface on the XenDesktop Delivery Controller (DDC) serve. The latest version of PowerShell that comes with Windows Server 2008R2 or later is required. For information on configuring PowerShell for use with the xendesktop probe, see the xendesktop Guide.
* Windows Remote Management (WinRM) enabled on the DDC server. For instructions on enabling WinRM, see the xendesktop Guide.

Prerequisites for the Xendesktop Probe

The probe can remote collect from the Xendesktop environment just like the VMware probe.

The Xendesktop probe requires the following software environment:

* Microsoft .NET Framework 3.5 on the system where the Infrastructure Manager application is running Important!: On 64-bit Linux systems, the Java jre included in the xendesktop probe package does not install successfully when you deploy the xendesktop probe on a CA Nimsoft robot. You must manually install the glibc.i686 library or compatible 32-bit libraries on 64-bit Linux systems where you deploy the xendesktop probe.
* Important!: On 64-bit Linux systems, the Java jre included in the xendesktop probe package does not install successfully when you deploy the xendesktop probe on a CA Nimsoft robot. You must manually install the glibc.i686 library or compatible 32-bit libraries on 64-bit Linux systems where you deploy the xendesktop probe.

## **Install the PowerShell Snap-In for xendesktop**

Install the PowerShell Snap-In (McliPSSnapIn.dll) using the Provisioning Server console installer.

If the Snap-In later needs to be registered in PowerShell, run *one*of the following commands at the DOS command prompt:

THIS IS AN IMPORTANT STEP TO DETERMINE THAT THE POWERSHELL SNAP IN HAS BEEN REGISTERED.

**Note:** Modify these commands to refer to the location of the Installutil.exe file in .NET Framework on your system and McliPSSnapIn.dll file in the Citrix folder on your system.\

**For 32-bit**

%systemroot%\Microsoft.NET\Framework\v2.0.50727\installutil.exe "C:\Program Files (x86)\Provisioning Services Console\McliPSSnapIn.dll"

**For 64-bit**

%systemroot%\Microsoft.NET\Framework64\v2.0.50727\installutil.exe "C:\Program Files\Citrix\Provisioning Services Console\McliPSSnapIn.dll"

You can also register the Snap-In by running *one*of the following commands at the PowerShell command prompt:

**For 32-bit**

$installutil = $env:systemroot + '\Microsoft.NET\Framework\v2.0.50727\installutil.exe';&$installutil 'C:\Program Files (x86)\Citrix\Provisioning Services Console\McliPSSnapIn.dll'

**For 64-bit**

$installutil = $env:systemroot + '\Microsoft.NET\Framework64\v2.0.50727\installutil.exe';&$installutil 'C:\Program Files\Citrix\Provisioning Services Console\McliPSSnapIn.dll'

## **Configure WinRM and PowerShell for xendesktop**

**WinRM on the DCC must be enabled and configured properly!**

WinRM on the DDC must be enabled and properly configured for use with the XenDesktop Monitoring probe. The XenDesktop Monitoring probe also requires remote unrestricted, unencrypted execution of PowerShell commands on the DDC. The PowerShell commands must have direct access (with valid user credentials) to the data store.

**Also check to make sure the port is correct. The port number is listed under Default Ports in the output for the previous step. The default is 5985.**

The xendesktop probe requires Windows PowerShell and Windows Remote Management (WinRM) to be enabled and properly configured on the XenDesktop Desktop Delivery Controller (DDC) server. You can use an HTTP connection type for WinRM, or, if you are using SSL to connect to the DDC, an HTTPS connection type.

**Follow these steps:**

**Note**: If any of the following commands having single quotations fail, then try to run the command without the quotation marks.

1. If the DDC server is running Windows Server 2008 R2, you must enable WinRM:
	1. As the Administrator user, go to the Control Panel and click **Add/Remove System Components**.
	2. Add **WinRM**under the section **Management and Monitoring Tools**.

Steps to Validate Configuration is correct.

## **Below are steps that will validate that Powershell and WinRM are configured properly.**

1)      Set Execution Policy

 

2)      Ran winrm quick config



3)      Set auth to basic



4)      Set to allow unencrypted



If you are using encryption you will need to refer to the Xendesktop probe documentation. It is also important to note that this document does not cover Multi-Hop Authentication.

If SSL is used for communication between the robot system and the DDC, configuration of WinRM on the DDC to use the HTTPS connection type. You will need the keystore location and keystore password to enter in the XenDesktop Monitoring probe Edit Resource dialog.

## **Security Validation**

**Verify PowerShell Access for xendesktop**

If the xendesktop probe cannot connect to the XenDesktop server, it may be because remote access to PowerShell on the XenDesktop DDC server is restricted. Verify that the correct access is set for PowerShell on the DDC server.

**Follow these steps:**

1. Open a PowerShell window on the DDC server and enter the following command:

**Get-ExecutionPolicy**

If the response says **Restricted**, you must change the setting to **Unrestricted**or **RemoteSigned**. For example, to set it to **RemoteSigned**:

* 1. Enter the following command:

**Set-ExecutionPolicy RemoteSigned**

* 1. Enter **Y** to accept the policy.
	2. Enter the **Get-ExecutionPolicy**command again to verify the setting.

If you are using Kerberos Authentication you will need to follow these steps.

Important! For Kerberos authentication to work, in Create New Resource dialog box, only hostname should be given.

Follow these steps:

1. Determine the file realm name by running the following commands on the XenDesktop Server machine.
	* echo %userdnsdomain% - Realm
	* echo %LOGONSERVER% - KDC name
2. Go to the probe directory and rename the krb5-TEMPLATE file to krb5.conf.
3. **Update the krb5.conf file with the file realm name and KDC name.**

**Example:**

In this example, the file realm name is ASC-FORWARDINC.COM and the KDC name is asc-ad.

[libdefaults]

default\_realm = ASC-FORWARDINC.COM

default\_tkt\_enctypes = RC4-HMAC DES-CBC-MD5 DES-CBC-CRC

default\_tgs\_enctypes = RC4-HMAC DES-CBC-MD5 DES-CBC-CRC

udp\_preference\_limit = 1

[realms]

ASC-FORWARDINC.COM = {

kdc = asc-ad.ASC-FORWARDINC.COM

}

[domain\_realms]

**.**asc-forwardinc.com = ASC-FORWARDINC.COM

asc-forwardinc.com = ASC-FORWARDINC.COM

1. Verify that the XenDesktop Server and probe machines are in the same time zone, and the time-difference between the machines is less than 5 minutes.

Important! The Kerberos Authentication mechanism might fail if the machine time is not set correctly.

## **Another Example File krb.conf**

[libdefaults]

 default\_realm = CHMCCORP.CCHMC.ORG

 default\_tkt\_enctypes = RC4-HMAC DES-CBC-MD5 DES-CBC-CRC

 default\_tgs\_enctypes = RC4-HMAC DES-CBC-MD5 DES-CBC-CRC

 udp\_preference\_limit = 1

[realms]

 CHMCCORP.CCHMC.ORG = {

 kdc = mccorpdc1.chmccorp.cchmc.org

 }

[domain\_realms]

 .chmccorp.cchmc.org = CHMCCORP.CCHMC.ORG

 chmccorp.cchmc.org = CHMCCORP.CCHMC.ORG

If you are still having problems after verifying that all of the xendesktop prerequites are met and the Xendesktop that you are attempting to monitor has been configured properly, see if your Xendesktop administrator can locate a log file from the Xendesktop you are attempting to monitor to determine why the probe login might be failing.

You can try to test from another workstation to server.  This will help to validate the Xendesktop Server is set up properly, if the probe is having issues connecting.

                

Configuring the Probe



Note: In the documentation it says the one of the accounts has to be a local admin user. This is not necessarily true. In fact the only way we were able to successfully connect is to set up the same domain admin user for both logins. The local admin may only be needed if the Xendesktop server exists in a separate domain.

Metrics from Xendesktop in the UMP

Note: the Xendesktop probe will not display metrics for the Citrix VDI desktops in the UMP, you will need to extract the data in the listviewer to see data.