**CloudPlatform**



Self Service Desktops

Installation Guide

  
www.citrix.com

Introduction

This document describes how to install the Citrix Self Service Desktops solution. The solution builds on work by Christian Ferber.

Objectives

CloudPlatform is a comprehensive cloud management solution which includes self-service capabilities. Many customers want to leverage self-service functionality for their virtual desktop installations to provide a portal where the user can select the desktop flavor he requires. In addition it should give the users more control over their desktops like start, stop, reboot, console access, network attach, attach ISO, attach volumes, console access and more. At the same time the performance to access the desktop should be optimal – hence XenDesktop with HDX capabilities should be used.

Overview

This document covers the following topics:

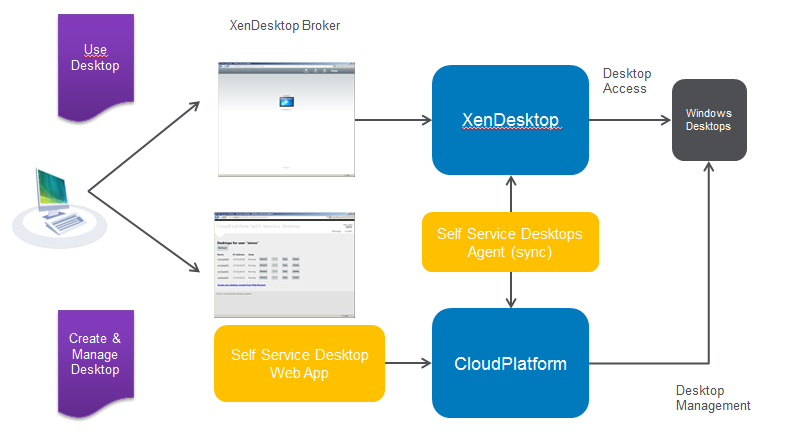
1. Architecture Overview of the solution
2. Preparation of the XenDesktop environment
3. Preparation of the CloudPlatform environment
4. Installation of PowerShell Active Directory integration
5. Installation of the Citrix Self Service Desktops solution.

Once the Self Service Desktops solution is installed there are two follow on documents to assist you in preparing the system to use:

* Sysprepped desktops – each new desktop will run the Microsoft Setup utility to prepare a brand new instance of the operating system [reference 1]
* Streamed desktops – Citrix Provisioning Services is used to stream a desktop image for each newly provisioned desktop [reference 2]

Architecture

The Citrix Self Service Desktops solution provides a simple way for end users to self-provision desktops. Desktops are hosted in Citrix CloudPlatform, HDX access to the desktop is provided by Citrix XenDesktop.



The diagram illustrates the overall architecture of the solution. The Citrix Self Service Desktops Web App provides a simple, intuitive web UI to allow a desktop user to create desktops on demand, power manage the desktops, and delete desktops that are no longer required.

Under the covers a Citrix Self Service Desktop Agent synchronizes between CloudPlatform and XenDesktop – as the user creates a new desktop the Citrix Self Service Desktop Agent will register it in XenDesktop; conversely when the user deletes a desktop, the Citrix Self Service Desktop Agent will remove the references from XenDesktop. The user may then access the desktops via the XenDesktop web interface.

Preparation of the XenDesktop environment

Obviously a XenDesktop installation is required for this functionality. As there’s no difference to a default XenDesktop installation this part is not covered in this article. Please refer to the official XenDesktop installation for more information on how to setup XenDesktop. The configuration has been tested with XenDesktop 5.6 but should work with other versions as well as long as they offer the same PowerShell API.

CloudPlatform VMs will be integrated as “unmanaged desktop” into XenDesktop which means that XenDesktop more or less only acts as broker instance and does not care about the desktop deployment itself (CloudPlatform task).

Preparation of the CloudPlatform environment

For CloudPlatform widely a standard installation can be used. Though there are a couple of configuration options which need to be considered to enable integration with XenDesktop

CloudPlatform API access

Make sure that CloudPlatform API is enabled for port 8096. This is done in the global settings of the CloudPlatform configuration and requires you to subsequently restart the cloud-management service (service cloud-management restart)



You may also need to configure the CloudPlatform Management server to allow incoming requests on TCP ports 8096 by editing the iptables file.

1. On the Management Server run the command:

vi /etc/sysconfig/iptables

1. Add this line

-A INPUT -p tcp -m tcp --dport 8096 -j ACCEPT

1. Save and exit the file and restart the iptables service using the command:

service iptables restart

CloudPlatform network configuration

The Citrix Self Service Desktops solution will not work with isolated networks in advanced zone. This is because XenDesktop requires direct access to the desktops; in CloudPlatform isolated networks there is a NAT enabled virtual router in the way which prevents XenDesktop communicating with the virtual desktops. As a result this solution requires either

* A shared network (VLAN) in Advanced Zone
* The default network in Basic Zone.

The most important point is that XenDesktop can reach the virtual desktops and vice versa, so the shared network in the advanced zone has to be routable to the network where XenDesktop and Active Directory reside.

In addition the “real” client (PC, laptop) accessing the virtual desktop needs to have direct access to the desktop as well as in a default configuration the communication is established directly. When using Access Gateway or NetScaler as ICA Proxy, it’s not mandatory to reach the shared network from the client directly, though AG/NS are required to reach it.

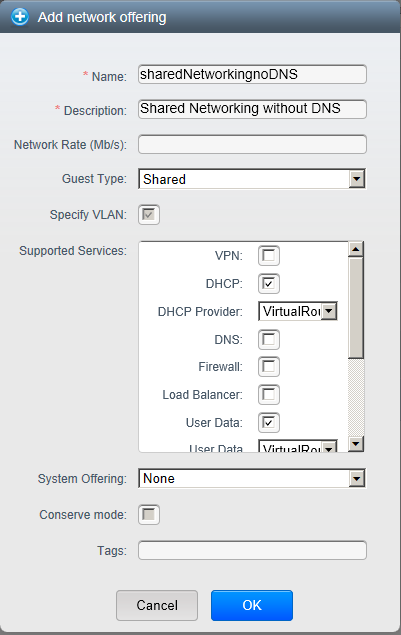
Create Advanced Zone Shared Network

This section gives some step by step instructions for creating a suitable shared network in an Advanced Zone. There are many different possible network topographies that can be used so this should be regarded as a sample only to guide you – it is not intended to be prescriptive.

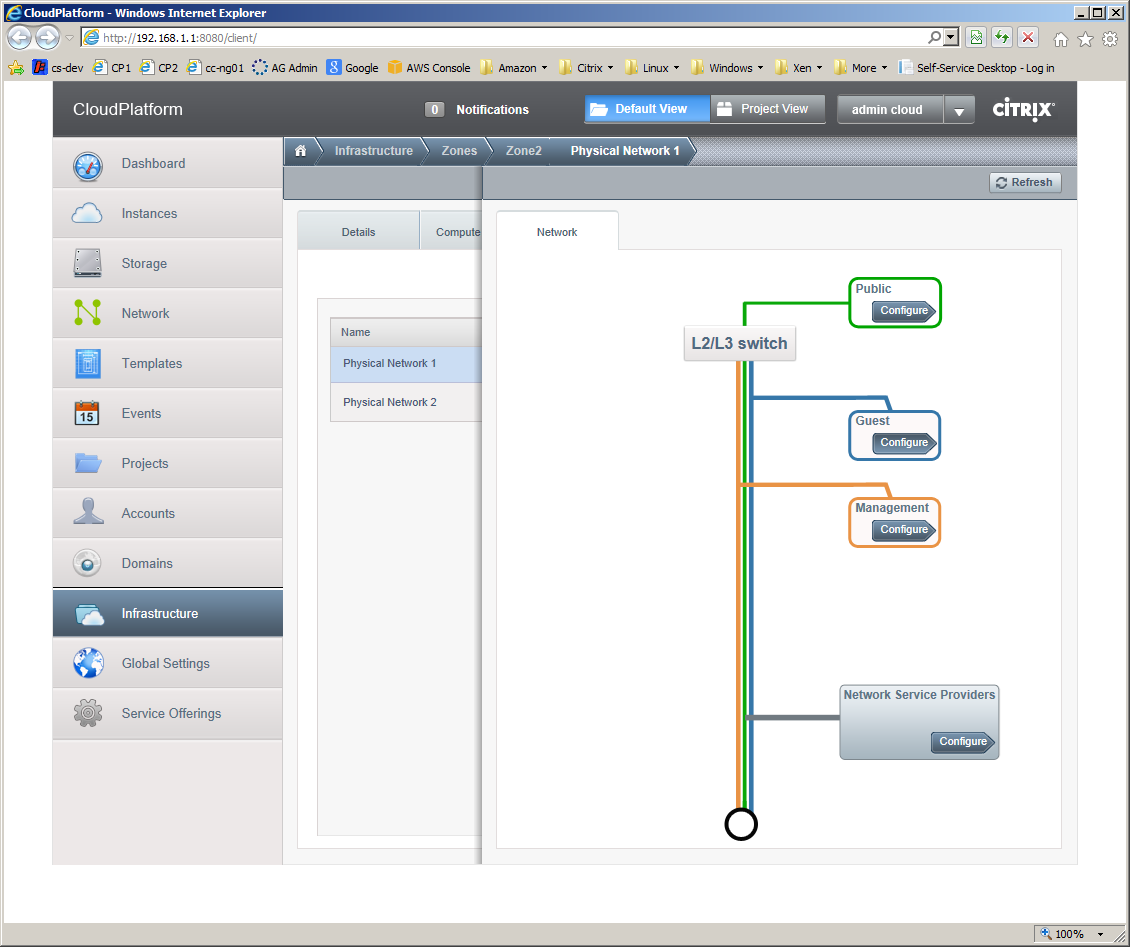
We will assume that CloudPlatform will just be used to host the self-service desktops. The XenDesktop Controller; Active Directory and optionally the PVS Server reside outside the cloud (either as physical or virtual servers). Also the client access devices deployed for the end users are outside the cloud. This is illustrated below



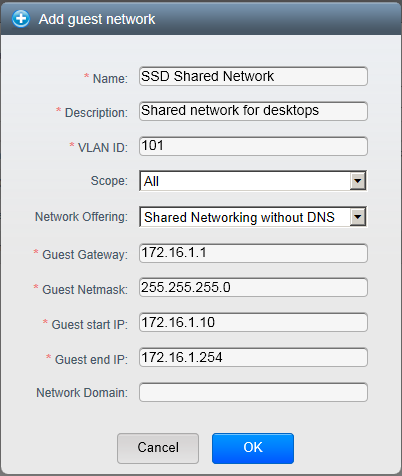
In the default configuration the CloudPlatform network offering for shared networks include DNS service for the router. As the DNS service does not forward tags required for AD authentication, AD integration won’t work using this network offering. Hence a new network offering has to be created which does not include DNS service. Use the CloudPlatform console to create a network offering for shared networks which does not include the DNS Service, as illustrated below:



Once you have created this network offering, then (as a CloudPlatform administrator) navigate to the CloudPlatform console for adding a guest network as shown here:



Click on the **Guest** / Configure button and the select the Network tab and then click on the **Add Guest Network** button to add a new network using the newly created network offering as shown below.



For a shared network you will need to designate a VLAN ID as shown, plus choose a range of IP addresses[[1]](#footnote-1) for use in the shared network. CloudPlatform will configure your XenServer with a network for the specified VLAN. You must also configure your network so that the non-CloudPlatform resources you are deploying (e.g. XenDesktop Controller, Active Directory and client machines) can route to this VLAN.

Active Directory integration of CloudPlatform

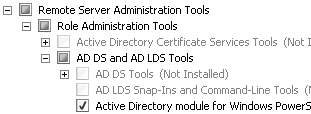
To enable self-service desktops you have to make sure that the user accessing self-service (CloudPlatform) uses the very same credentials to access XenDesktop as well as CloudPlatform. This requires CloudPlatform to be integrated in the active directory domain. To do this step, please follow the guide ‘Setting up AD Authentication in CloudPlatform [reference 3]’.

Note that the AD users are not automatically imported into CloudPlatform; hence it’s required to create each user that should have self-service capabilities in CloudPlatform. We recommend creating the user with an IT defined complex password which is not known by the user himself. This is because CloudPlatform requires a password for each user created but is able to authenticate through active directory when the corresponding user is available in AD. There is always the option to login as well using the IT defined CloudPlatform password for the user. For a production installation there could be a PowerShell script which syncs users from AD to CloudPlatform (not in the scope of this solution)

Install PowerShell module for Active Directory

As the solution requires access to Active Directory and needs to be able to read and write data, it’s required to have the PowerShell module for Active Directory installed on the XenDesktop delivery controller.

The module can be activated in the Windows server manager as part of a feature installation:



For Windows 2003 and 2008 domain controllers you also need to install Active Directory Management Gateway Service.

Installation of Citrix Self Service Desktops

The overall Citrix Self Service Desktops solution is currently packaged as two MSI files for easy installation on Windows. Both applications should be installed on the XenDesktop Controller:

* Citrix.SelfServiceDesktops.Agent.Setup.msi
* Citrix.SelfServiceDesktops.WebApp.Setup.msi

Prior to installation, create a directory named C:\CtxLogs – this is where diagnostic logs from the solution will be written.

Install the Agent first. This will typically install into a folder named C:\Program Files (x86)\Citrix\SelfServiceDesktops\Agent. In this folder is a configuration file named Citrix.SelfServiceDesktops.Agent.exe.config – you will need to define you site’s configuration.

The recommended approach to managing your sites configuration is to use the Citrix Self Service Desktops Administration tool (see reference 4), but if you wish you may edit the configuration file using your chosen editor (it is an XML document). A sample configuration file for the Agent is included in Appendix A.

If you edit the configuration file manually, you will need to restart the Citrix Self Service Desktop Agent – from a command prompt type services.msc to get the Windows Services administration console to do this.

Once the Agent is installed, you should install the web; this will use the configuration defined for the Agent. The web app will install to http://<server>/Citrix/SelfServiceDesktops**.** A sample configuration file for the web app is included in Appendix A, but normally you will not need to change this, as all the web app configuration is imported from the agent.

After that, you are ready to go. The Agent should look after itself (check **C:\CtxLogs** for any error messages if you encounter problems)

Troubleshooting

|  |  |
| --- | --- |
| Problem | Action |
| Self Service Desktop Agent fails to start | The Agent will perform a sanity check of the configuration file when it starts up. If it detects any problems with the configuration; it will log an error in C:\CtxLogs\self-service-desktops-agent.log and exit. Check the log file and correct any configuration errors. |
| HTTP Error 403.14 – Forbidden when you try to access the Web App | Typically this is caused by a problem with ASP.NET Routing on Windows 2008. The problem is fixed in Service Pack 1, so we recommend installing that. For more information, and alternative solutions if you do not wish to install Service Pack 1see reference [5]. |

References

1. Self Service Desktops with Sysprep
2. Self Service Desktops with PVS
3. Setting up AD Authentication in CloudPlatform
4. Self Service Desktops Administration Guide
5. [Configuration Settings for ASP.NET Routing](http://msdn.microsoft.com/en-us/library/cc668201.ASPX#configuration_settings_for_routing)

Appendix A – Sample Configuration Files

Sample Agent Configuration

The Agent configuration defines all the settings for both the Agent and the web app. We recommend using the Self Service Desktops Administration Tool to manage these settings but you may also edit the XML if required.



Sample Web App Configuration

Under normal circumstances the web app imports all of its configuration from the Agent as illustrated by the following configuration file section (this is in the Web.config file of the web app).



However, if circumstances make importing the Agent configuration problematic, you are able to clone a full <selfServiceDesktops> element within the Web.config file. If you do this you must make sure that it is consistent with the Agent configuration.

1. Clearly the address range you choose for the shared network must be compatible with your existing network. [↑](#footnote-ref-1)