

Terminal Services 2008 Design Document

For

Family Credit
Technopolis
Kolkata



Ontrack House,

19, Ekdalia Road,

Kolkata – 700019, India

Telephone: +91 33 2460 1980/1/2 /2129

Fax: +91 33 2460 1280

Web Site: www.ontrackindia.com

E-mail: info@ontrackindia.com

Date: 16th September, 2008

1. Executive Summary

1.1 Purpose of the document

The purpose of this document is to provide an overview of the planning and design for setting up terminal services infrastructure based on windows server 2008 at the office of Family Credit, Kolkata. This document also includes various Microsoft recommendations and best practices for Terminal Services implementation at Family Credit.

2.0 Planning Checklist

1. Hardware and Software requirements.
2. Planning Terminal Services role configuration.
3. Planning Terminal Services Session Broker configuration using TS Farm.
4. Planning Network Load Balancing configuration.
5. Planning Terminal Service Gateway role configuration.
6. Planning Terminal Services Licensing Server.
7. Tuning up terminal server.

2.1.1 Hardware and Software Requirements

Hardware- Two nos. Sun Fire x4150 server hardware will be used for installing and configuring terminal services, terminal services web access and terminal services remote application roles and one DELL Optiplex desktop will be acting as terminal services session broker server and terminal services gateway server.

Software-Family Credit will provide all software licenses required for setting up Terminal Services 2008 infrastructure.

- For setting up TS gateway, TS session broker and core Terminal Services role, we need windows server 2008 Standard x32 Edition OS.

2.1.2 Planning Terminal services role configuration

Terminal Services, a presentation virtualization technology delivered as a core component of Windows Server 2008, enables anywhere, anytime access a full Windows desktop or a server running Windows-based programs, from almost any computing device. Users at Family Credit can connect to the terminal server to run their line of business applications and can use network resources on that server. This core terminal service component will be installed and configured on each SUN Fire x4150 server hardware using load balancing technology in a terminal services farm. Both the servers will be running windows

server 2008 standard x32 as the primary operating system. These servers should be member of an active directory domain.

Key features like terminal services web access and terminal services remote application will be installed as a part of terminal services role and configured in both the servers eliminating single point of failure. TS Remote Application provides access to remote programs or LOB applications through terminal services. To the end users, programs will appear as if they are running on their local desktops, including resizable windows, drag and drop support between multiple monitors, and notification icon in the notification area. Users can run these remote programs side by side with their local programs. Internal users as well as branch office users at family Credit will be accessing their LOB applications using an .rdp file that will be installed on their local machine. An icon or shortcut will be visible at each end user's desktops and users will just need to double-click on that icon and connect to the terminal server located at their head office. Users will not have to manually start the Remote Desktop Client to start remote application programs.

Users will also have the option of accessing their remote programs through web browser using TS web Access component of Windows server 2008. TS web access enables users to launch a connection from the web browser to the remote desktop of the terminal server where they have appropriate access.

All client machines from where users will be connecting the terminal server should have RDC 6.1 (remote desktop client) installed. RDC 6.1 includes the ActiveX control required to access TS web access. It is included in Vista SP1 and Windows XP SP3 by default.

2.1.3 Planning Terminal services Session Broker configuration using TS farm

Terminal services session broker role will be installed on a Dell Optiplex desktop machine with 2 GB RAM running windows server 2008 standard x32 as the primary operating system. The server should be member of the same active directory domain. This role will keep track of disconnected sessions and allow users to reconnect to an existing session in a load-balanced terminal server farm. TS session broker will store session state information that includes session IDs and their associated user names, and the name of the server where each session resides.

Terminal services session broker service will start automatically after TS session broker role installation and creates a group named Session Directory Computers local group. This group is not populated by default. The terminal servers participating in the TS session broker farm needs to be made members of this group.

Both the servers configured with Terminal Services role will be members of the terminal services farm. Session load will be distributed equally among these two servers by assigning relative weight value to each server. Relative weight Value, a TS session broker load balancing feature, is the value assigned to distribute the load between more powerful and less powerful servers in a farm. TS Farm name will be

same for both the servers and will be used by TS session broker to determine which servers are in the same terminal server farm.

Members of terminal services farm communicates with TS session broker to ensure that users are transparently reconnected to the original server hosting their disconnected sessions. This happens in a two-way process-

1. When a user logs on to the terminal server farm, the terminal server receiving the initial client logon request sends a query to the TS session broker server.
2. The TS session broker server checks the user name against its database and sends the result to the requesting server. One of the following occurs:
 - If the user has no disconnected sessions, logon continues at the server hosting the initial connection.
 - If the user has a disconnected session on another server, the client session is passed to that server and logon continues.

2.1.4 Planning Network Load Balancing configuration

Network Load Balancing will be used as the load balancing technology for distributing network traffic across the servers by using the TCP/IP networking protocol. Using NLB with terminal server farm helps to scale the performance of a single terminal server by distributing sessions across multiple servers. Advantage of deploying NLB along with TS session broker load balancing is that both the network-based load balancing and failed server detection of NLB can be achieved.

Two nos. network interface cards needs to be installed on each SUN Fire x4150 server hardware. One no. will be used for communicating with clients and other servers. The other one will be used for private communications (load balancing) between these two servers. Only TCP/IP will be enabled on this NLB adapter.

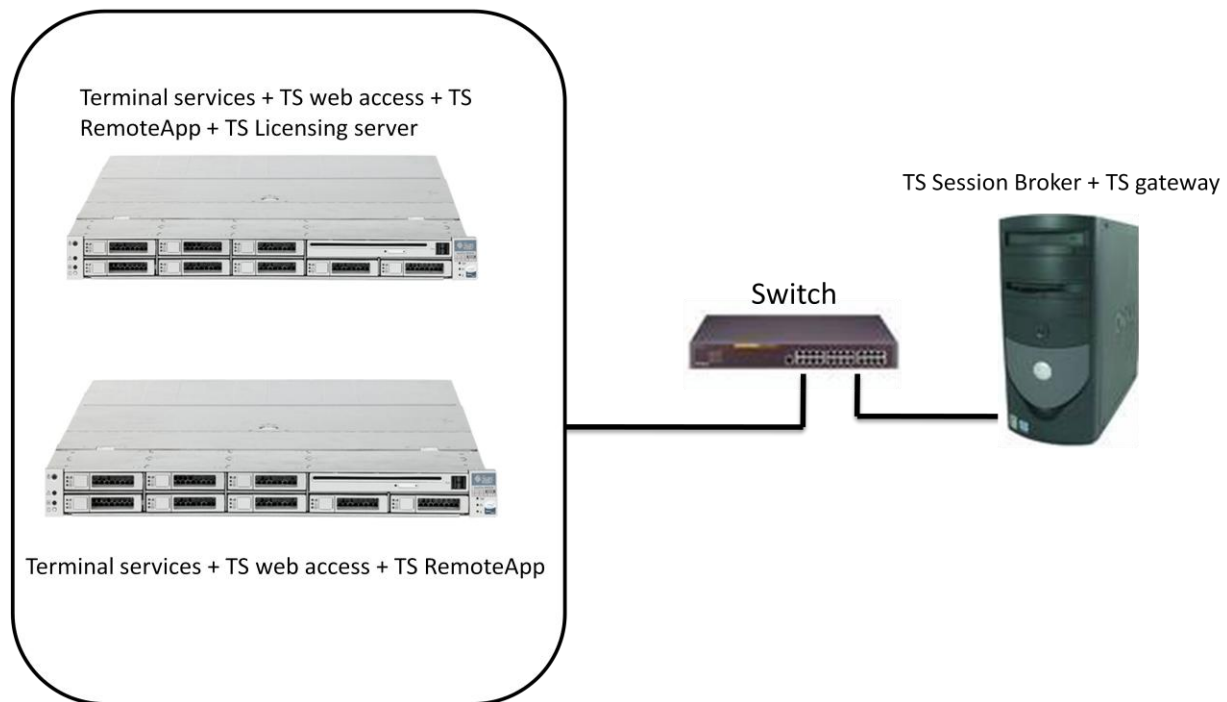
User account needed to install and configure NLB must be member of the Administrators group of that server.

2.1.5 Planning Terminal services gateway role configuration

TS gateway role will be installed on the same DELL Optiplex hardware with TS session broker role. TS gateway will enable authorized remote users at FC to connect to resources on the corporate network by encapsulating Remote Desktop Protocol within RPC, within HTTP over a secure sockets layer (SSL) connection. TS gateway will generate and use a self-signed certificate for this encrypted communication. Authorization policies will be created using TS gateway manager to define conditions that must be met for remote users at FC to connect to the internal resources. Terminal services connection authorization policies (TS CAPs) allows to specify user groups that can access a TS gateway server. A separate group needs to be created in existing active directory and remote users who will be connecting to the terminal server must be made members of this group. TS CAPs will allow only this group to connect to the

terminal server through this TS gateway server. Terminal services resource authorization policies (TS RAPs) allows to specify the network resources (computers) that remote users can connect through a TS gateway server. A separate computer group will be created and servers acting as terminal servers will be made members of this group. This group will be associated with TS RAPs for allowing users to connect remotely to the servers through TS gateway.

TS FARM



2.1.6 Planning Terminal services Licensing role configuration

One no. Sun Fire x4150 server hardware will be configured with terminal services licensing role. TS licensing server will be configured in Per-Device mode and responsible for providing licenses to each device that will be accessing the terminal servers. Each device CAL permits one device used by any user to conduct windows session on any of the terminal servers. These device CALs are distributed to the client device and the license is presented for validation at every connection. This license server should be able to connect to the activated license server in order to issue permanent licenses to the client device else it will only issue temporary licenses.

2.1.7 Tuning up Terminal services

To speed up the performance, each terminal services role needs to be tuned. Terminal services gateway performs many packet forwarding operations between TS client instances and TS server instances

utilizing some amount of network bandwidth. To reduce bandwidth utilization by TS gateway, certain registry parameters needs to modified. Other tuning parameters for improving terminal service performance includes-

- i) Setting page file size to custom instead of system managed.
- ii) Disabling screen saver and password protected screen saver.
- iii) Disabling UAC.
- iv) Forcing windows to start using classic start menu.
- v) Disabling certain MS win32 services.
- vi) Disabling CEIP program and windows Error reporting.
- Vii) Disabling redirection of devices like clipboard, audio, drives etc.

For server details and IP details refer to [FC_Design.xls datasheet](#).