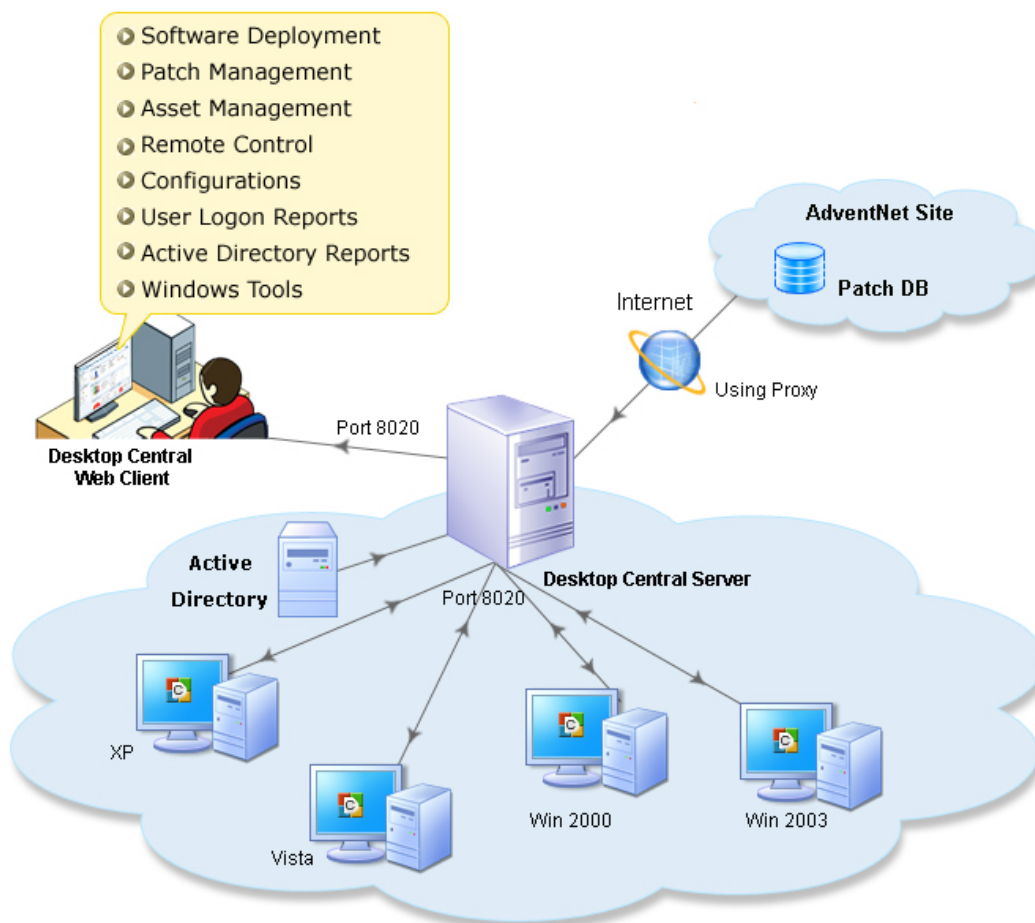# Desktop Central LAN Architecture

Desktop Central Architecture

Overview

ManageEngine Desktop Central is Web-Based windows desktop administration software that helps administrators to effectively manage the desktops from a central point. It provides Software Deployment, Patch Management, Service Pack Installation, Asset Management, Remote Control, Configurations, System Tools, Active Directory Reports and User Logon Reports.

The figure below depicts the Desktop Central Architecture. The details of the individual components are given below:

Desktop Central LAN Architecture

ZOHO Corp.

Desktop Central Architecture

Server Component

Desktop Central Server is located at the enterprise (customer site) is responsible for performing various Desktop Management activities. It pushes the Desktop Central agent to the client machines, deploys configurations, initiates scanning for Inventory and Patch Management, and generates reports of the Active Directory Infrastructure Components to effectively manage the desktops in the enterprise network. It is advised to keep the Desktop Central server always running to carry out the day-to-day Desktop Management activities. All these actions can be initiated from a web-based administration console in a few simple clicks.

Agent Component

Desktop Central Agent is light-weight software that gets installed in the client systems that are being managed using Desktop Central. It acts as a worker to carry out the operations as instructed by the Desktop Central Server. It is also responsible for updating the Desktop Central Server with the status of the deployed configurations. The agent periodically pulls the instructions from the Desktop Central Server and executes the tasks. The agent contacts the server at the following intervals:

1. For user-specific configurations - during user logon and every 90 minutes thereafter till the user logs out of the computer.
2. For computer-specific configurations - during system startup and every 90 minutes thereafter till the system is shutdown.

Patch Database

The Patch Database is a portal in the ManageEngine site, which hosts the latest vulnerability database that has been published after a thorough testing. The Desktop Central Server periodically synchronizes this information and scans the systems in the enterprise site to determine the missing patches. Subsequently, the patches are installed to fix the vulnerabilities.

Desktop Central Architecture

The communication between the Desktop Central Server and the Patch Database is through the Proxy Server or a direct connection to internet. The required patches will be downloaded from Microsoft website and stored locally in the Desktop Central Server before deploying the patches to the client computers. Hence, each client computer (agent) will take the patch binaries from the Desktop Central Server

Web Console

- ❖ Provides a central control point for all the desktop management functions.
- ❖ Can be accessed from anywhere: LAN, Remote Offices, and Home through Internet/VPN.
- ❖ No separate client installations are required.

Active Directory

For Active Directory based Domain setup, the Desktop Central Server queries the Active Directory to generate out-of-the-box reports for Sites, Domains, Organization Units, Groups, Computers, etc., which gives you a complete visibility into the Active Directory.

Ports Used by Desktop Central

The Desktop Central server uses different ports to communicate with the agents to enable them to complete tasks related to desktop management.

Ports to be Opened on the Agent:

To enable remote installation of the Agent, you should open these ports.

135 : Used to enable remote administration.

139 & 445 : Used to enable sharing of files and printers.

Desktop Central Architecture

Ports to be Opened on the Server:

8020: Used for agent-server communication and to access the Web console

8383: Used for secured communication between the agent and the Desktop Central server

8443: Used to control computers remotely(secure mode)

8444: Used to share computers remotely

8031: Used to transfer files in a secure mode

8032: Used to transfer files

8027: Used to complete on-demand tasks like inventory scanning, patch scanning, remote control, remote shutdown and moving agents from one remote office to another