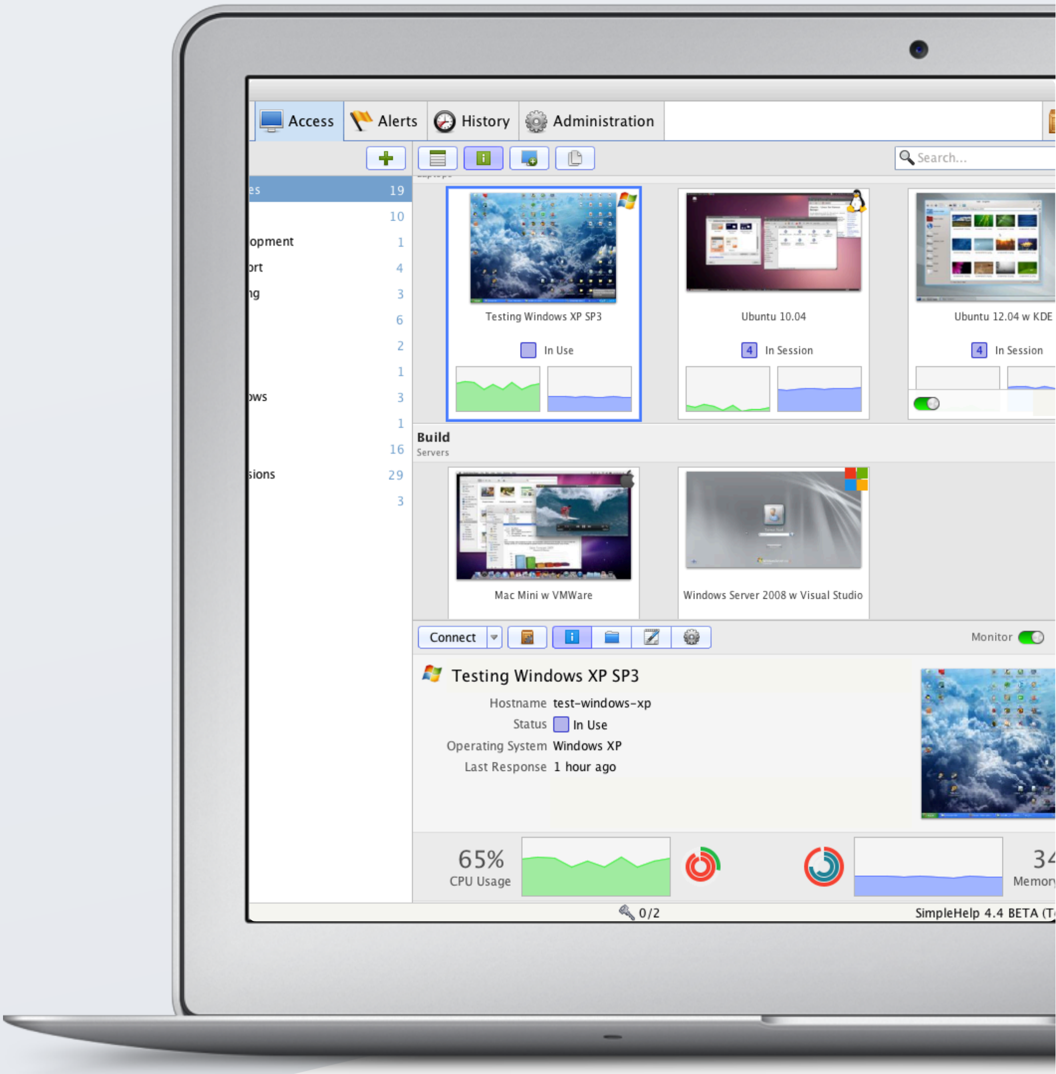
simplehelp

TECHNICAL AND ARCHITECTURAL BRIEFING



Testing Windows XP SP3

Hostname test-windows-xp
Status In Use
Operating System Windows XP
Last Response 1 hour ago

TABLE OF CONTENTS

OVERVIEW

SELF HOSTED REMOTE SUPPORT, ACCESS AND MANAGEMENT SOLUTION

SimpleHelp gives Technicians the ability to provide live on-demand support sessions to remote users in need by allowing them to view and control the user's remote computer. Technicians can also install a Remote Access Service on desired systems to access these systems unattended without any remote user interaction, and can manage large groups of remotely accessible systems to monitor them live, set alerts to be notified of issues, and perform mass maintenance on groups of machines.

SIMPLEHELP SERVER

The core of your SimpleHelp installation is the SimpleHelp web server. This is the central point of contact handling:

- Distribution of Technician, Customer and Access applications (linked to your server)
- Proxying of connections between support customers, access machines and Technicians to avoid onerous firewall changes
- Gathering and storage of all data from monitored and alerted remote access services.

SimpleHelp server is a dedicated web server which handles only the small subset of web queries required to serve applications and allow them to communicate. It does not rely on Apache or IIS and does not support dynamic scripting of any kind, keeping the potential attack surface to a bare minimum and greatly simplifying ongoing maintenance.

APPLICATIONS

For users, the core of the SimpleHelp experience lies with the applications downloaded from the SimpleHelp server:

- Remote Support for users requesting live assistance
- Technician for support representatives helping users live and managing maintenance of systems
- Remote Access for installation of the Remote Access Service for unattended Technician access and management

SERVER INSTALLATION AND REQUIREMENTS

HOST ON ANY PLATFORM YOU ARE COMFORTABLE WITH

SimpleHelp Server can be installed on any of Windows, Linux or MacOS and can be run on physical hardware or a virtual server with dedicated allocated resources.

Rather than being forced to learn a new skill set or hire in outside expertise you can use infrastructure that you are already comfortable with and SimpleHelp will fit right in.

Every part of SimpleHelp is architected with scalability in mind, both from a machine resources and a network perspective.

The exact scalability of your server will depend on a number of factors including how it is used. The sections below should be treated as guidelines and where possible a trial should be set up to establish scaling based on your typical usage.

Terminology: one hyperthreaded CPU core = two CPU threads, recommendations assume dedicated assigned cores

SERVER CPU REQUIREMENTS

- Minimum one cpu thread, two or more always recommended to minimise latency.
- Under 10 sessions, 500 services, most non-free-tier 1GB+ VPS systems are sufficient, 2+ cpu threads is best. Free tier systems often have no dedicated resources and can introduce latency.
- Above this, one physical dedicated cpu thread will typically support 50+ very heavy use sessions, 100+ light use sessions, 2500+ services. Multiple servers may be required for large deployments (see the Clustering section for more details).
- Given the variability of resource allocation on some virtualised systems we recommend installing a trial to ensure system suitability. VPS systems with no dedicated/guaranteed resources can introduce latency.

SERVER MEMORY REQUIREMENTS

- 1GB minimum
- Under 20 sessions, 2000 services - 2GB minimum
- Under 100 sessions, 5000 services - 8GB minimum
- Over 100 sessions, 5000 services - 16GB minimum, ability to scale to 32GB

NETWORK REQUIREMENTS

- Idle sessions use approximately 0.5k/sec, 2-3k/sec for diagnostics, typically sessions will include idle periods with bursts of usage based on screen changes on the remote machine
- 1000 machines UDP - approximately 35k/s (45k/s with monitoring)
- 1000 machines HTTP - approximately 100k/s (200k/s with monitoring)

HIGH AVAILABILITY FAILOVER AND CLUSTERING

HIGH AVAILABILITY FAILOVER

SimpleHelp is capable of registering a secondary, tertiary or more (if required) failover servers to act as a live backup to your primary server.

In cases where maintenance is required, Technicians can be notified of an impending switch to a secondary server. Technicians may then postpone the switch while they complete important work, subject to a timeout policy set by the server admin, upon which they will be forcibly switched to the failover server.

Sessions are reestablished for both support customers and Technicians providing minimal impact for both during the transition and allowing very high levels of availability of your SimpleHelp system.

Remote access services can be shared with many servers to provide as much failover capacity as you wish.

CLUSTERING

SimpleHelp server is able to scale to access, monitor and alert over very large numbers of computers.

Machines shared with UDP place minimal strain on the SimpleHelp server and can be shared directly with it always, giving a simple, easy to maintain architecture.

For deployments where HTTP or even HTTPS are required by policy or firewall or proxy rules, SimpleHelp can handle large numbers of remote access services by the deployment of one or more Auxiliary services which act to handle much of the network load, forwarding the relevant requests to the Central, Primary server.

SECURITY AND AUTHENTICATION

INDUSTRY STANDARD PROTECTION - AES-256 - DTLS - LETS ENCRYPT SSL

SimpleHelp converges on one mechanism to secure data transferred between technicians and customers or technicians and remote access services. In doing this we focus on one secure implementation that is then used across multiple apps and multiple forms of encapsulation.

SimpleHelp implements a protocol effectively DTLS using AES-256, RSA-4096, and a combined 256-bit SHA-512/SHA3 (Keccak) authentication hash. Since SimpleHelp always retains control over both ends of the connection (app + server) SimpleHelp deviates from the DTLS specification only to avoid negotiating these algorithms (and the downgrade attacks this attracts) and encapsulate across multiple possible transport layers. All sessions and established communications between a remote access service and your server will therefore always use AES-256 and RSA-4096.

Whether you are connected in a session using HTTP, TCP or UDP as an underlying transport or accessing a remote machine's stats or filesystem, all communications are encrypted using this protocol and these mechanisms.

Although SimpleHelp does support and can use SSL, SimpleHelp does not rely on SSL connections to provide security except in the case of browser sessions such as the mobile client (/mobile page on your server) and secure presentations being viewed in a browser. SSL can be configured but this is not necessary for the data transferred to be encrypted and in practice SimpleHelp will be performing DTLS encapsulated over the underlying SSL connection. SimpleHelp will always use its DTLS based protocol with its enforced encryption algorithms (RSA-4096 / AES-256) and will treat the base level connection purely as a transport, much in the same way that SSL will treat TCP/IP as a transport.

As such even when connected to the remote machine over SSL SimpleHelp will still encrypt all information transferred with its standard high security algorithms and will not simply rely on SSL to provide a secure layer. This approach allows SimpleHelp to establish connections via a variety of mechanisms including plain HTTP, TCP, SSL and UDP while retaining high security across all.

Established connections therefore may appear to use plain HTTP or TCP but this is a result of encapsulating the secure DTLS implementation on top of these.

For true simplicity in setting up security for your mobile and presentation access, your SimpleHelp server supports Lets Encrypt automated certificate requests and renewals leaving you with zero ongoing work and costs to manage your SimpleHelp server SSL certificates.

AUTHENTICATION

SimpleHelp server is capable of integrating with a wide variety of existing authentication mediums including support for redundant authentication servers in enterprise environments.

SimpleHelp Technician authentication supports:

- LDAP / ActiveDirectory authentication, both of specific tech accounts and of users without a corresponding SimpleHelp technician account, defined only within LDAP / AD
- RADIUS authentication
- Multi factor support, including app or email one time passwords
- Restriction of user permissions and rights based on membership in LDAP / ActiveDirectory