Cloud PBX Solutions

Cloud PBX Core

System Requirements

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT THE SELLER REPRESENTATIVE FOR A COPY.

Introduction

Ensuring all the necessary components is essential when deploying a cloud PBX platform. This page provides general hardware and virtual infrastructure requirements for various components of the cloud PBX platform. Note that these requirements may vary depending on specific tasks, goals, and the set of functionalities.

Hardware Requirements

We recommend using high-performance server hardware supporting 64-bit architectures and suitable processors for this type of system.

Supported hardware platforms:

- Intel X86-64
- IBM z/Series (also requires the presence of Intel X86-64 nodes for handling media streams).

Supported operating systems:

- Debian GNU/Linux 9 and later
- Red Hat Enterprise Linux 8.0 and later
- Fedora Linux 28 and later
- IBM z/LinuxONE.

Supported virtualization environments:

- Linux KVM
- VMware ESXi
- IBM z/VM
- OpenStack.

This page provides an example server configuration for a standard set of components of the cloud PBX platform, designed for 7500 users and a call load of 5 CAPS (Call Attempts Per Second) with 300 CC (Concurrent Calls).

The platform supports scalability (both vertical and horizontal by increasing the hardware power of nodes and adding new nodes) at all stages of project growth: users, traffic, and other parameters.

Accounts	Number of Servers Without Redundancy	Number of Servers With Redundancy	Server Specifications
7500	1	2	CPU: 2x Intel Xeon CPU E5-2620 v4 RAM: 96GB DDR4 RAID: HW SAS with support for RAID1 + BBU on supercapacitors SSD: 2x 256GB HDD: 2x 2Tb SAS Network: 2x Gigabit Ethernet

Requirements for VMware Virtual Machines

- The Latency Sensitivity option must be enabled for VM centrex-* (fe/be/mg) with a setting of "High" (minimum for the MG).
- Failover support must be ensured for all virtual machines in the cluster.

- There should be an option to disable VM backup using virtualization platform tools.
- Resource reservation for VMs on the host (CPU/memory reservation) is established.
- The VM migration mechanism between hosts during high node loads (vMotion) is disabled.
- A VLAN is configured among all virtual machines.

The total volume of resources for virtual machines with reservation for a standard cluster configuration, designed for 7500 users and a call load of 5 CAPS (Call Attempts Per Second) with 300 CC (Concurrent Calls).

CPU	MEM, Gb	DISK, Gb
44	144	4000

The platform supports horizontal and vertical scaling of virtual machines without interruption in the service.

Limitations

We recommend using the latest versions of virtualization software to ensure optimal performance and security. Regular updates of the host OS and hypervisors are conducted on our side.

Network Requirements

Minimum Requirements:

- Bandwidth: 1 Gbps.
- Latency: Less than 5 ms.
- Quality of Service (QoS): No less than 99.9%.

Recommended Requirements:

- Bandwidth: 1 Gbps or higher.
- Latency: Less than 1 ms.
- Quality of Service (QoS): No less than 99.99%.

Dedicated network resources and devices supporting QoS are recommended to ensure the high performance and reliability of the platform. When deploying the platform in a virtual infrastructure, compliance with the supported virtualization platform requirements and the availability of the necessary number of network interfaces is essential.

Security Requirements

General security requirements:

- Firewall policies: everything not explicitly allowed is forbidden.
- Access to the system and critical data must use personal accounts with limited privileges, accessed via a cryptographic key.
- External network connections should be secured with TLS protocol using a minimum key length of 2048 bits.
- Access control mechanisms must be used to grant access only to necessary information for each user or user group.
- Regular backups of all critical data and system settings and testing recovery procedures after an emergency are necessary.
- Monitoring system logs and security events is essential to detect potential threats or attacks.

Recommendations for security settings and monitoring potential vulnerabilities or threats:

- Timely update software and system patches to avoid vulnerabilities.
- Use intrusion detection systems and event monitoring to respond promptly to threats.
- Conduct security audits and vulnerability scans regularly to identify potential weaknesses or risks.
- Ensure the physical security of servers hosting the cloud PBX platform.
- Regular user training on information security and social engineering will increase awareness and vigilance.