Chime for Teams Machine and System Requirements

Machine:

Instant Chime works well with standard physical or virtual machines and may be installed on common platforms including: Microsoft HyperV, Microsoft Azure, Amazon AWS, Google.

Base machine specs:

# Queues	RAM	Processor	File System	Database Size
1 to 5	8 GB	1-2 Core	100 GB	1 GB
5to 20	12 GB	2-4 Core	200 GB	2 GB
20 +	16 GB	4 Core	200 GB	3 GB

If hosted through Microsoft Azure, use a Standard D1 v2 (1 vcpu, 3.5 GiB memory) or greater for the Virtual Machine and a Standard S3: 100 DTUs Database

OS and Overview:

- 64-bit Windows Server: 2012, 2012 R2, 2016, and 2019
    - Server 2008 R2 requires Desktop Experience feature to be installed
    - Server 2012/2012 R2, and 2016 require Media Foundation feature to be installed
- Instant Chime **does not** require Microsoft IIS since Instant Chime includes HTTP via OWIN

Database Connectivity:

Database access and connection to Microsoft SQL Server or Microsoft SQL Express (typically SQL Express used during evaluation not for production instances).

- Account with create access to SQL server (for building and updating the Chime database)
- Account with read\write access to Chime database
    - The application supports both SQL and Windows server authentication options.
    - *Note:* For optimal performance, Chime and SQL Server should be in the same physical site.

Additional Information:

Chime (Self hosted) with Office 365 and Microsoft Teams support

- .Net Framework 4.7.1+
- Configured Azure Active Directory application registration for Graph API access (see Chime Office 365 Prerequsites.pdf)
- 1+ Bot Framework registered bots per queue
- Microsoft Teams subscription
- 1 SSL Certificate (.pfx format)
- Publicly available hostname/ip address

Graph API Permissions:

API / Permissions name	Type	Description	Admin consent required
AppCatalog.ReadWrite.All	Delegated	Read and write to all app catalogs	Yes
Channel.ReadBasic.All	Application	Read the names and descriptions of all channels	Yes
Directory.Read.All	Application	Read directory data	Yes
Presence.Read.All	Delegated	Read presence information of all users in your organization	No
Team.ReadBasic.All	Application	Get a list of all teams	Yes
TeamMember.ReadWriteNonOwnerRole.All	Application	Add and remove members with non-owner role for all teams	Yes
TeamsApp.ReadWrite	Delegated	Manage user's Teams apps	No
User.Read	Delegated	Sign in and read user profile	No
User.ReadBasic.All	Delegated	Read all users' basic profiles	No

Hostname and Firewalls

The Chime server will need to have a publicly addressable DNS hostname and **public IP address** in order for Microsoft Bot Framework to be able to deliver Teams chat messages to the Chime server.

Additionally, it will be necessary to allow incoming traffic on **port 443 (HTTPS).**

It is not currently possible to provide specific IP address ranges that would need to be whitelisted for incoming requests for Bot Framework requests, as Microsoft does not make that information available and it may change at any time.

SSL Certificate

To set up a Chime for Teams deployment, you will need to acquire a SSL certificate. This certificate will be installed on the same server that the Chime instance will be deployed on. Without this certificate installed, no users will be able to authenticate into the web app. Self-signed certificates won't work, Certificates should be from a valid SSL issuing authority like: GoDaddy, Thawte, Symantec etc...

The certificate must have a **Subject** and **Subject Alternate Name** which matches the public hostname of the Chime application server, as will be configured for the Reply URL in the Azure AD Application Registration in Azure. For the easiest setup, please acquire a certificate in the .pfx format as it will make adding it much easier.

It is recommended that a **Signature algorithm** of at least **sha256RSA**

The certificate should have an **Enhanced Key Usage** property of **Server Authentication (1.3.6.1.5.5.7.3.1)**