Vivoh OnTime For Zoom

Architecture and Server Configuration

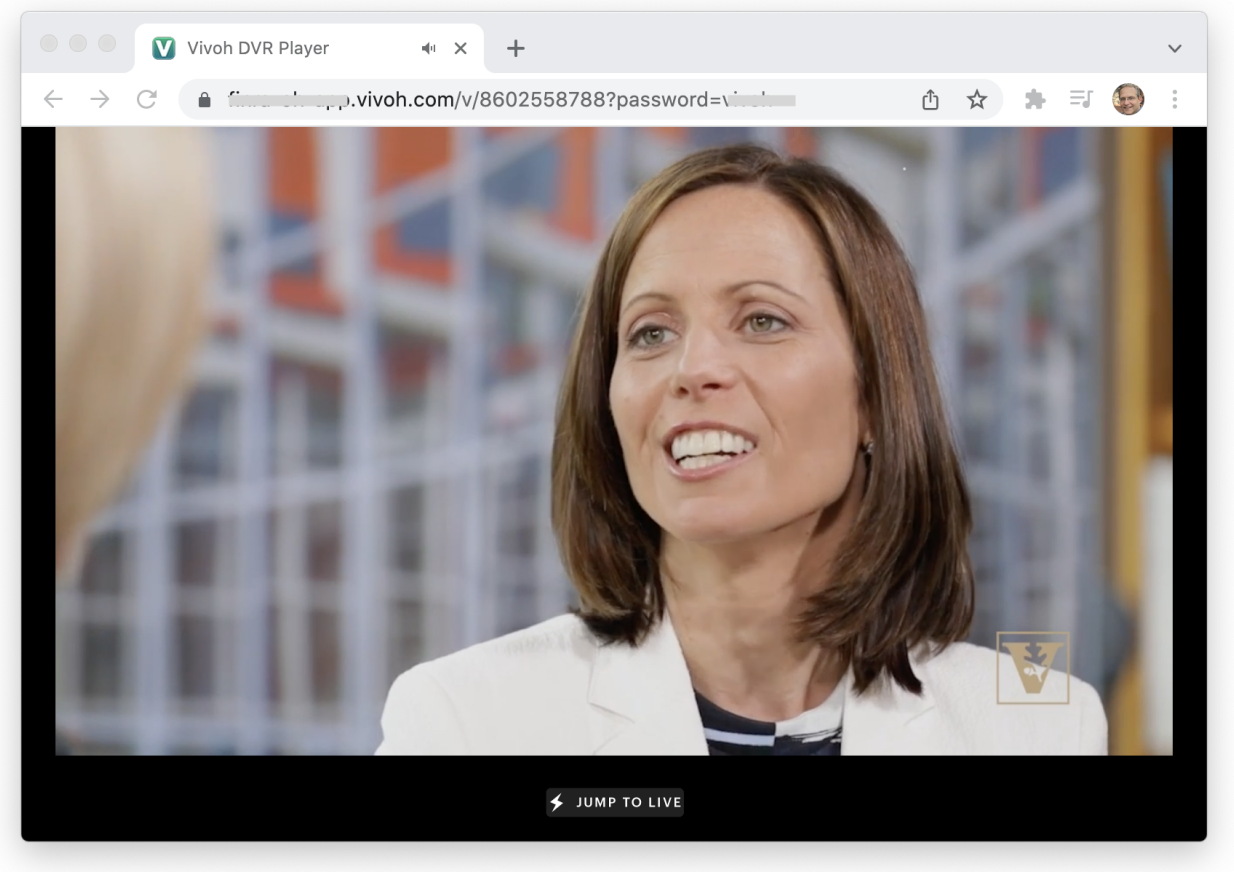
Contents:

1: Introducing Vivoh OnTime For Zoom

Vivoh OnTime for Zoom is a “DVR for meetings” service which extends Zoom meetings with pause, rewind, and 2X playback capability during the live meeting. Now hosts can start every meeting on time since attendees can catch up on their own when they arrive. Now attendees can show up late and catch up without disrupting the meeting or they can pause the meeting if they need to take another call or take a break and then quickly catch back up. Non native speakers can rewind and playback content at ½ speed in order to understand it more easily.

Vivoh OnTime has a simple, web-based, user interface which works well with modern browsers on Windows, MacOS, or Linux desktops as well as Android and iPhone mobile devices.

Hosts configure their Zoom meeting streaming settings to point to the Vivoh OnTime servers. Authentication is via Zoom which supports single-sign-on (SSO), Google, and Facebook logins or SSO via OKTA. Hosts may set a password for each Vivoh OnTime meeting and/or add a list of allowed attendees for authorization. Vivoh OnTime can be configured to restrict access to users with approved email domains, for example from your company.

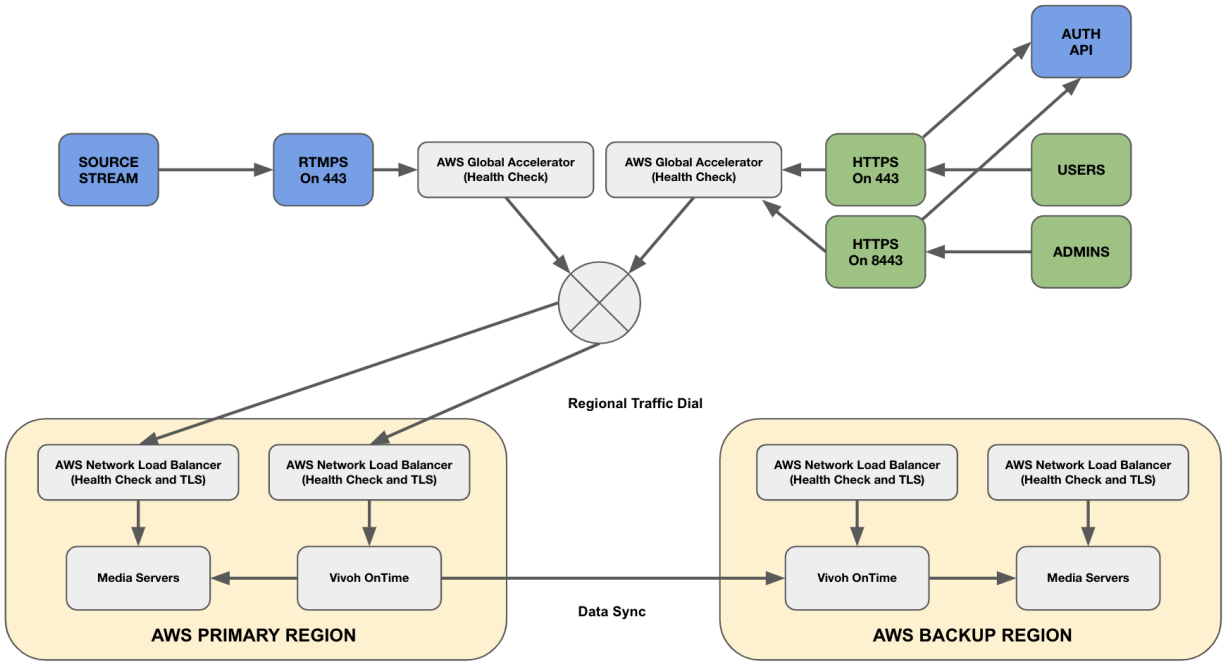


2: Vivoh OnTime Architecture

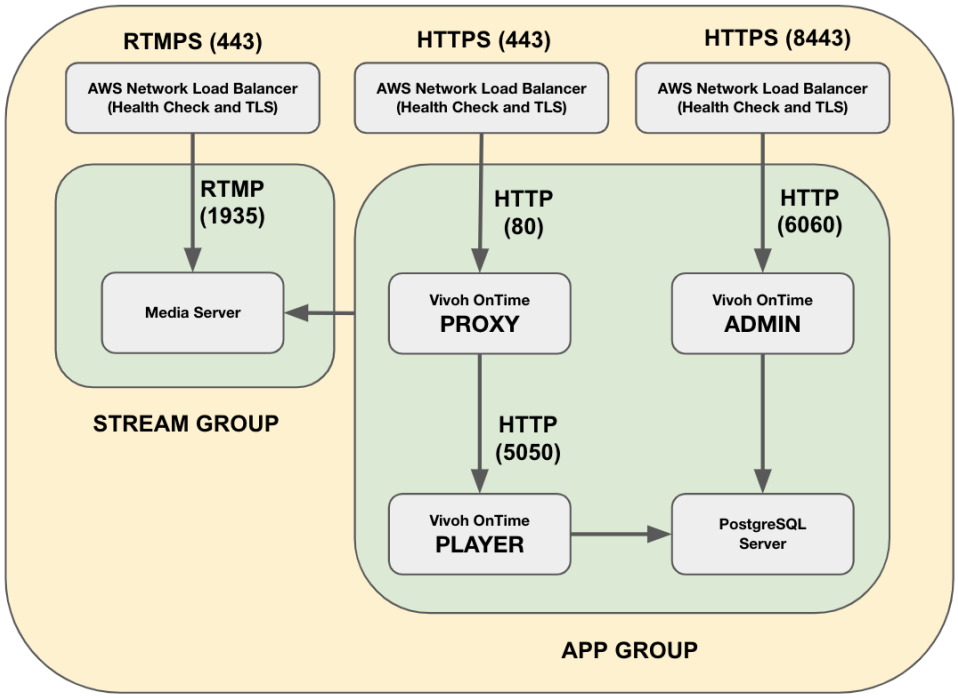
Vivoh OnTime For Zoom is a web based application that displays the live video content from a Zoom meeting within a standard video-on-demand playback interface. This lets the user pause, rewind, and change the speed of video playback. No software is required for both hosts and attendees other than a browser.

Vivoh OnTime For Zoom requires authentication via a Zoom Marketplace App that is installed by each user or by a customer-specific SSO configuration. Authentication enables Vivoh OnTime to trust the identity of the user. The user's email address is then used for authorization, including access to the Vivoh OnTime Meeting Manager, per-domain user access across all meetings, or per-meeting access from a customer-provided list of attendees.

Hosts configure Zoom to push live video of their meeting to the Vivoh OnTime servers, which are typically deployed in the Amazon or Microsoft hosting environments. Vivoh OnTime server software can also be deployed in other hosting environments and both Linux or Windows on premises servers. A best practice is to deploy Vivoh OnTime with regional redundancy and load balancing with automatic scaling. The following is a diagram for an existing Vivoh customer, where Vivoh is managing their high availability deployment in AWS.



Vivoh OnTime For Zoom servers include media servers for video streaming, web servers for the user and administrator interfaces, a proxy that implements security, and a database.



Vivoh OnTime includes a patent-pending method for enhanced security whereby no video data is stored as files on disk rather this data is buffered in memory on the server-side. All data is encrypted in transit and delivered via HTTPS. Video from Zoom is encrypted and ingested securely via the RTMPS protocol.

Vivoh extends this security with on premises Vivoh Video Caching Proxy servers. The Vivoh OnTime data buffer is replicated locally while retaining the same level of security. These servers can deliver the content to thousands of users behind your internet gateway, reducing your circuit costs and protecting your firewalls from being overloaded.

Additional security measures include a per-meeting password and several authentication and authorization options. Users are authorized via Zoom or a SSO provider and one option is to restrict access globally to a specified set of authorized email domains.

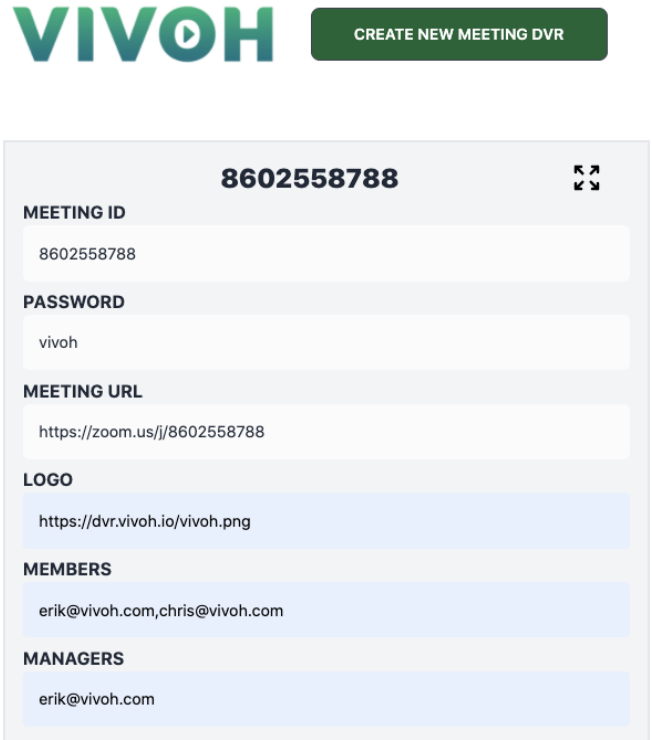
Vivoh will configure at least one **Manager** that is authorized to create new meetings. Authorized **Managers** can authorize additional authenticated users to configure the password and **Member** list for a specified meeting.

3: Configuring Authentication and Authorization

Vivoh OnTime enforces authentication for users and administrators via Zoom, which includes Zoom, Google, and Facebook logins and Zoom-configured SSO. Alternatively, Vivoh can configure SSO access via OKTA, SAML, or ADFS services. Once the identity of the user is verified, their email address is used for authorization.

Administrators are authorized via the OnTime server's *admin.ini* file when their email address is configured, like so: ADMINISTRATORS=erik@vivoh.com,admin@vivoh.com. **Administrators** can create new Vivoh OnTime meetings in the Meeting Manager and then can assign **Managers** for the meeting by listing their email addresses in the **Managers** field.

Attendees are authorized via the *proxy.ini* file which may include the following configuration option: MEMBER_DOMAINS=vivoh.com. This enables all authenticated users with an email address containing the vivoh.com domain to attempt to access the meeting. These users may be blocked if an **Administrator** or a **Manager** lists other email addresses in the **Members** field for the specified meeting but does not include them in this list. Further these users may be blocked if an **Administrator** or a **Manager** applies a password to the meeting that is unknown to these users.



4: How To Contact Vivoh

Vivoh can be reached on sales@vivoh.com or (860) 606-7878.

More information is available at https://vivoh.com/ontime.