TechNote – AltitudeCDN™ OmniCache Integration with Microsoft Teams Live Events

Version 1.0

AltitudeCDN^{TM} OmniCache is a robust proxy cache that enables the efficient delivery of HTTP Live Streaming (HLS) or DASH video content across the enterprise. OmniCache provides a flexible, scalable, and distributed platform that delivers high-quality low-latency video, while protecting and conserving limited enterprise Wide Area Network (WAN) resources.

OmniCache provides Microsoft Teams Live Event customers with a video caching solution for live meeting broadcasts.

This guide describes how to provision AltitudeCDN OmniCache for a Teams Live Event.

Contents

© 2018 · Ramp Holdings Inc. · All rights reserved.

Introduction

During Teams Live Events, large numbers of viewers each attempt to individually connect to external content delivery network (CDN) servers, creating a high demand on WAN network resources that can lead to congestion, poor video quality, and even service interruptions for event viewers or other network clients.

To avoid these issues, AltitudeCDN OmniCache provides local video-content caching features that can be configured to fully support Teams Live Events. By using OmniCache, retrieval of video content from external CDN servers is greatly reduced, and shared content is internally distributed to enterprise WAN clients. The flexibility of this approach allows you to properly engineer network bandwidth usage to avoid service degradation, and maintain a high-level quality of service (QoS).

The integration of OmniCache with Microsoft Teams Live Events consists of two parts:

- Traffic steering – OmniCache includes several mechanisms that allow you to steer requests for Teams Live Event video content to the appropriate OmniCache nodes in your environment.
- Content caching – OmniCache can be configured to recognize and store Teams Live Event video content, and efficiently deliver content to enterprise clients.

Requirements

To use AltitudeCDN OmniCache with Teams Live Event, you need the following:

Item	**Recommendation**
OmniCache	OmniCache v1.6.2 or later – The OmniCache must be installed and running on an on-premise Windows or CentOS platform, positioned within the customer network so traffic can reach both the audience and external video source. For more information, see the *AltitudeCDN OmniCache Deployment Guide*.
Traffic Steering Mechanism	You need either of the following: • A Proxy Auto-Configuration (PAC) file to indicate the IP address or DNS name of an appropriate OmniCache node. • Enterprise Domain Name System override for Teams Live Event video origin hostname.

© 2018 · Ramp Holdings Inc. · All rights reserved.

Solution Summary

Relevant HTTP requests from client browsers or video players for HLS and DASH video content are directed via PAC file or enterprise DNS name override to an appropriate OmniCache node. OmniCache's unique routing features can additionally provide request routing that re-writes manifests to distribute subsequent request loads across a scalable set of OmniCache nodes:

- If PAC file redirection is used, then OmniCache is configured in a standard forward-proxy mode.
- If DNS name override is used, then the OmniCache is configured as a reverse-proxy.
- In either case, the content is typically provided over HTTPS, so the OmniCache must be provisioned with a certificate that allows it to serve TLS/SSL traffic on behalf of the external CDN servers. Typically, this certificate is generated by an internal enterprise Certificate Authority (CA) where all potential viewers have been configured to trust that certificate.

PAC File – Forward Proxy

The example below illustrates PAC file syntax that directs Teams Live Event video content queries to an OmniCache node:

```
function FindProxyForURL(url, host) {
        if (dnsDomainIs(host, "endpoint1-prdeuscompsvc.streaming.mediaservices.windows.net")){
              return "PROXY <OmniCache IP>:<OmniCache Port>";
        }
        if (dnsDomainIs(host, "endpoint1-prdwuscompsvc.streaming.mediaservices.windows.net")){
              return "PROXY <OmniCache IP>:<OmniCache Port>";
        }
        if (dnsDomainIs(host, "endpoint2-prdeuscompsvc.streaming.mediaservices.windows.net")){
              return "PROXY <OmniCache IP>:<OmniCache Port>";
        }
        if (dnsDomainIs(host, "endpoint2-prdwuscompsvc.streaming.mediaservices.windows.net")){
              return "PROXY <OmniCache IP>:<OmniCache Port>";
        }
return "DIRECT";
}
```

Note: *You must ensure that the external CDN hostname is correct, otherwise the PAC file will not redirect the requests.*

Example Forward OmniCache Configuration

This example uses a standard forward configuration for PAC file override:

```
"proxyEngines": [{
                "port": 10200,
                "mode": "standard",
                "httpsCertificateNames":"*.streaming.mediaservices.windows.net"
        }],
```

See the *AltitudeCDN OmniCache Deployment Guide* and *AltitudeCDN OmniCache Reference Manual* for complete information on configuring OmniCache.

© 2018 · Ramp Holdings Inc. · All rights reserved.

DNS Name Override – Reverse Proxy

The example below illustrates how an internal DNS name override is used to steer relevant HTTP requests to an appropriate OmniCache node. The enterprise DNS administrator could create a CNAME record for `endpoint1-prdeuscompsvc.streaming.mediaservices.windows.net`, which has the value of an appropriate OmniCache node (for example, `master-omnicache.your-enterprise.com`). The internal enterprise DNS may have features that allow a different OmniCache node to be returned depending on the location of the requester. In reverse-proxy mode, the HTTPS requests are directed to port 443, by default.

Example Reverse Proxy OmniCache Configuration

This example uses a reverse-proxy configuration for enterprise DNS override:

```
"proxyEngines": [{
                "port": 443,
                "mode": "reversehttps",
                "httpsCertificateNames":["*.streaming.mediaservices.windows.net"],
                "uriRewrites":[
                {
                    "pathPattern":"/(.*)",
                    "hostPattern":"endpoint1-prdeuscompsvc.streaming.mediaservices.windows.net",
                    "pathReplacement":"/https/endpoint1-
prdeuscompsvc.streaming.mediaservices.windows.net/$1"
                }]
        }],
```

See the *AltitudeCDN OmniCache Deployment Guide* and *AltitudeCDN OmniCache Reference Manual* for complete information on configuring OmniCache.

Microsoft Teams Live Event Setup

Teams needs to be enabled for Live Events within your company administration account. Once Teams Live Events are enabled there is no special configuration is required to enable an event to be cached by OmniCache. See the following Microsoft documentation for information on scheduling a Teams Live Event:

`https://support.office.com/en-us/article/Schedule-a-Teams-live-event-7a9ce97c-e1cd-470f-acaf-e6dfc179a0e2`

© 2018 · Ramp Holdings Inc. · All rights reserved.

Certificate Management

As Teams Live Events use HTTPS delivery, installing a trusted CA certificate is recommended so OmniCache can decrypt, process, and cache HTTPS requests.

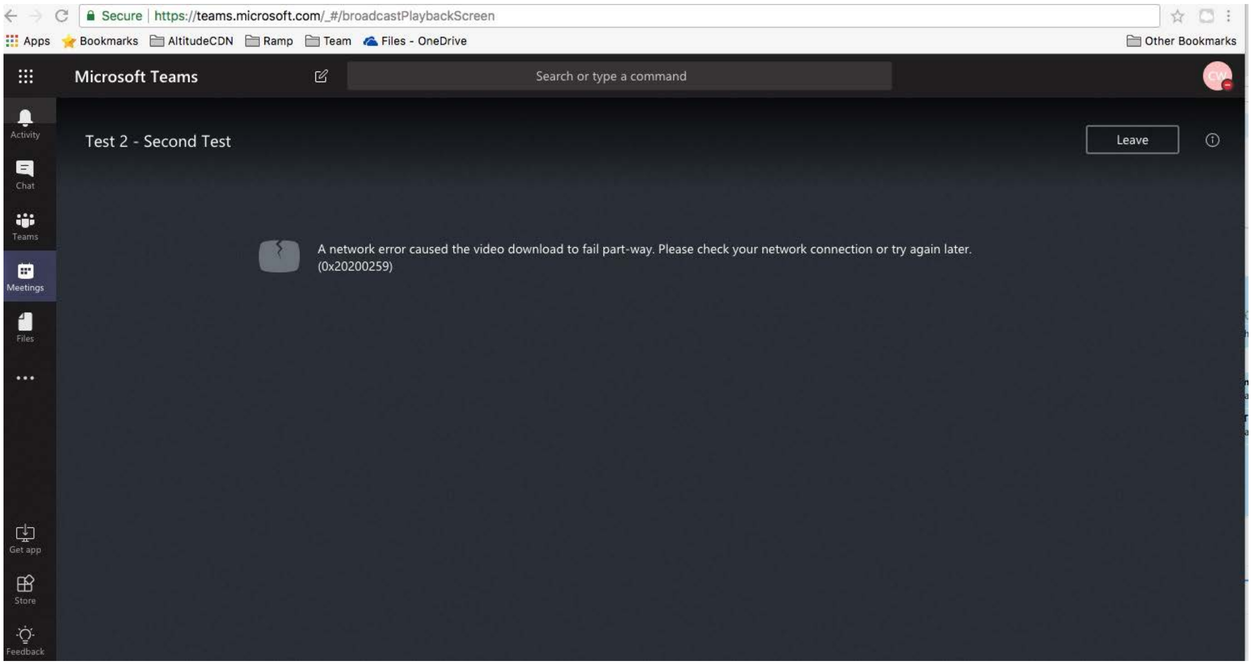
For information on installing a trusted CA certificate on an OmniCache running in reverseHTTPS mode, see the *AltitudeCDN OmniCache Reference Guide*.

Running OmniCache for Teams Live Events Without an HTTPS Certificate

While not recommended for production deployment, testing OmniCache with Teams Live Events can be performed without installing an HTTPS certificate.

To demonstrate that packets are being cached by OmniCache, do the following:

1. Configure OmniCache to run in reverseHTTPS mode, and either deploy the redirection PAC file, or use DNS redirect to your environment.
2. Schedule a Teams Live Event and publish it live.
3. Enter the event via a Web Browser as an attendee.
4. The event page crashes with the following error:



A network error caused the video download to fail part-way. Please check your network connection or try again later. (0x20200259)

5. Within the web browser's Developer Tools, go to the Network tab and look for the video manifest file. This file displays as red, as it is attempting to a connect to an HTTPS location without a certificate.
6. Copy the manifest URL to a new browser tab, which prompts an HTTPS security exception.
7. Accept the security exception.
8. Re-enter the event in the web browser as an attendee. The Teams Live Event video loads, plays, and is cached by OmniCache.

© 2018 · Ramp Holdings Inc. · All rights reserved.