Cloud Access Software

A security-compliant, multi-tenant virtual environment for the media and entertainment industry

This collaborative effort between Jellyfish Pictures, an award-winning visual effects and animation studio, Pixit Media and Teradici provides a reference architecture for production studios and design firms wishing to implement security-compliant multi-tenant virtual studio environments, offering unprecedented scalability in-city, nationwide and even internationally. Leveraging highly scalable enterprise storage from Pixit Media and ultra-secure PCoIP remote workstation access, the architecture offers a template for concurrent isolated virtual studios instantiated on a per-project basis, each studio meeting distinct production requirements in terms of staffing, compliance and infrastructure.

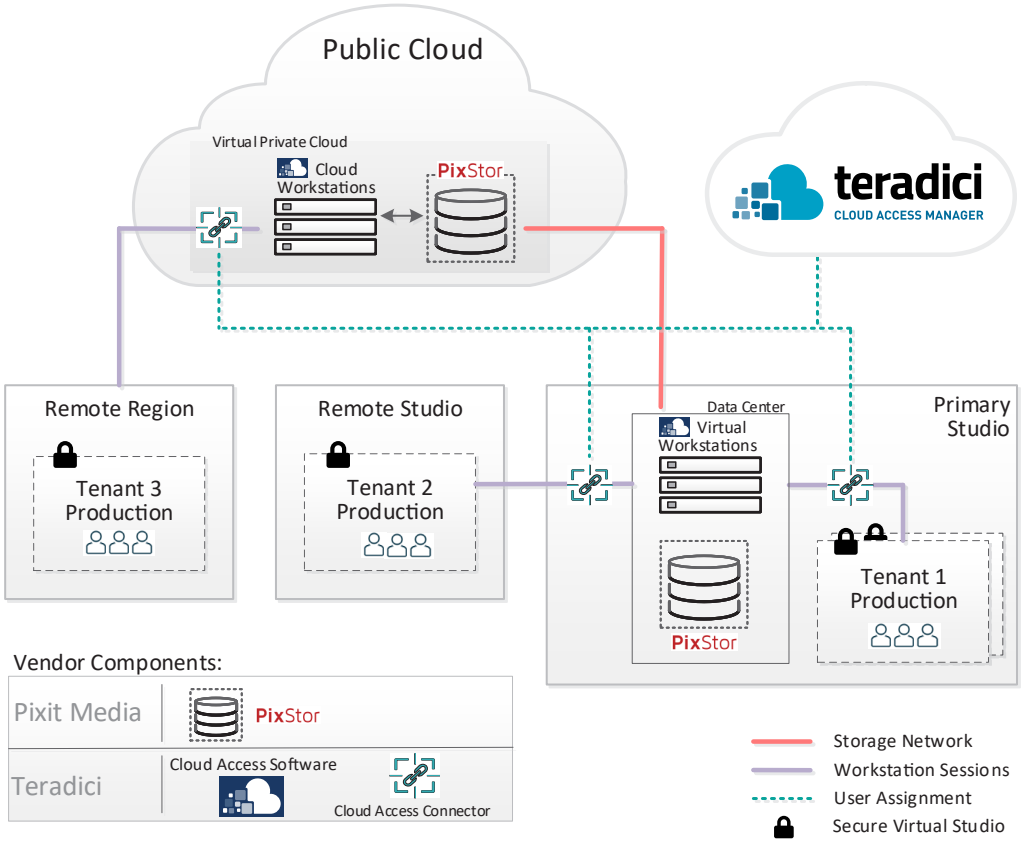
JELLYFISH PICTURES

pixitmedia

teradici

Solution Overview

The scalable virtual studio template is illustrated below. The primary studio has an on-premises data center or machine room with virtualized workstation and storage resources described in more detail below. The primary studio incorporates 'Tenant 1 Production' as a virtual studio facility staffed with editors and artists – typically a primary studio hosts several concurrent productions, each as a separate isolated virtual studio meeting specific compliance standards. Of course, the data center itself may be located on-premises or offsite based on preferred infrastructure arrangements. The PCoIP protocol provides the secure backbone for workstation sessions between artist and workstation across all configurations; Teradici Cloud Access Software generates an encrypted PCoIP pixel stream terminated by a compliant endpoint device such as a PCoIP Zero Client at the desk. Secured peripheral device communications including keyboard, mouse and pen tablet signals are transmitted back to the workstation, ensuring a near-native interactive environment for the artists. On-premises virtual workstations are supported by the PixStor software-defined storage platform while those in the cloud are serviced by PixStor Cloud instances which ensure that only necessary data is transferred to the cloud and cloud-generated data is proactively flushed back on-premises.



Scalable Virtual Studio Template

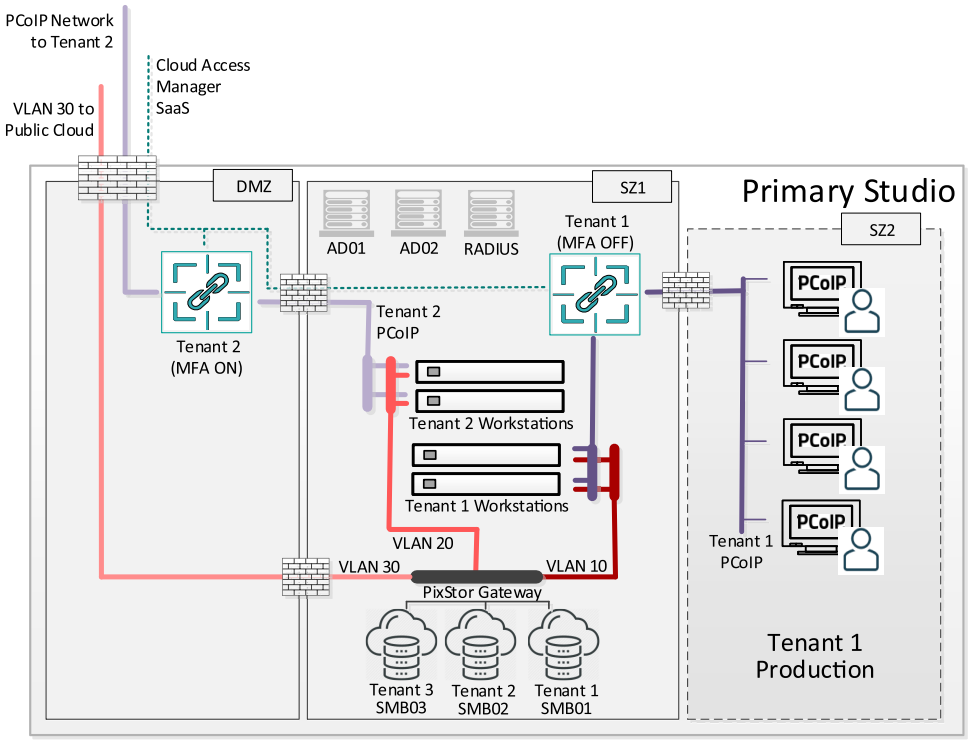
The deployment template above includes remote studio and remote region footprints. For architectural simplicity, the illustration shows a single remote studio supporting Tenant 2 Production but is scalable according to demand – for example Jellyfish Pictures have several facilities in the London area and one in Sheffield operating as remote studios, each supporting one or more productions. The remote studio

is served with virtual workstations and storage infrastructure hosted in the primary data center such that the remote studio itself has no Intellectual Property (IP) assets and is readily locked down. Similarly, the remote region hosting Tenant Production 3 is a virtual studio with no on-premises IP assets either but served with infrastructure from a Public Cloud Service Provider (CSP) rather than the private data center. This enables instantiation of virtual studios in any international region supported by the CSP within a virtual private cloud (VPC) subscription under a common set of security policies. Details regarding the role and configuration of storage network (shown in red) and the Teradici Cloud Access Manager SaaS service supported by Cloud Access Connectors (blue icons and dashed lines) are described in the section below.

Security and Compliance Elements

OVERVIEW

To meet Motion Picture Association of America (MPAA) published best practices and achieve Trusted Partner Network (TPN) compliance, it is mandatory to apply security controls to any assets classified as high security content. These controls include physical restrictions to on-premises and remote facilities in addition to infrastructure perimeter security measures, public internet isolation, separation of office and production networks and content management policies along tenancy boundaries so that concurrent productions can be managed according to governing security policies and procedures, which may differ from one production to another. The network configuration for the primary studio illustrated below shows the key isolation aspects.



Primary Studio Infrastructure

The primary studio incorporates a production network infrastructure in an isolated security zone SZ1 separated from a demilitarized zone (DMZ) comprising internet-facing gateways and one or more security zones (e.g. SZ2) designated as tenant production areas. Corporate infrastructure (not shown) is assigned to an independent security zone separated from SZ1 and SZ2.

PRODUCTION FLOOR ISOLATION

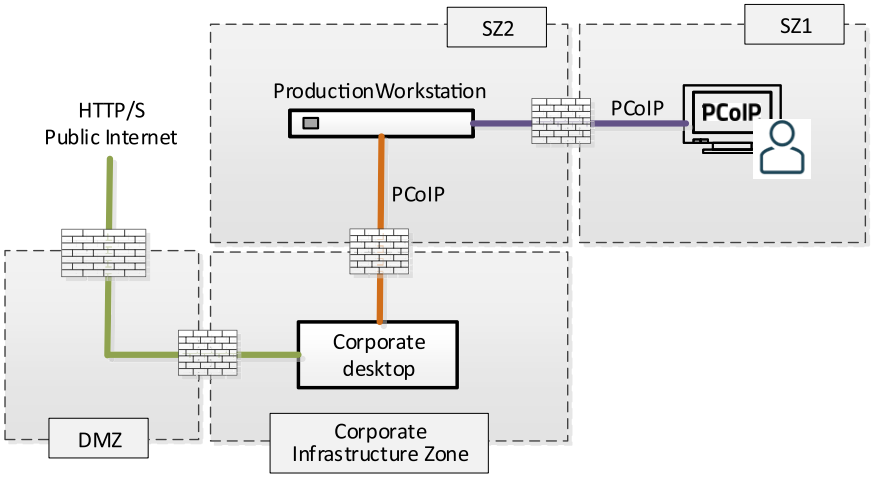
Artist stations in the production area are populated with PCoIP endpoint devices such as stateless Zero Clients or thin clients accompanied by monitors and peripheral devices such as pen tablets – this remote access architecture for all three tenants ensures that no high security content is present in local or remote production areas which dramatically streamlines security compliance in terms of asset management and digital security best practices.

SECURE WORKSTATION ACCESS

On-premises workstations are networked on a per-tenant basis and located in the security zone SZ1 isolated from both the production area and the DMZ. The Teradici Cloud Access Connector for tenant 1 in SZ1 brokers PCoIP connections between tenant 1 users listed in Active Directory (AD01) and tenant 1 workstations as assigned in the cloud based Teradici Cloud Access Manager. Likewise, a second Cloud Access Connector in the DMZ brokers PCoIP connections originating from external Tenant 2 in conjunction with a separate Active Directory (AD02). However, external users (Tenant 2 production) are authenticated by the Cloud Access Connector in the DMZ (using RADIUS-based multi-factor authentication (MFA)) to achieve compliance. The workstations assigned to each tenant are served by dedicated storage resources described below.

CORPORATE NETWORK AND INTERNET ISOLATION

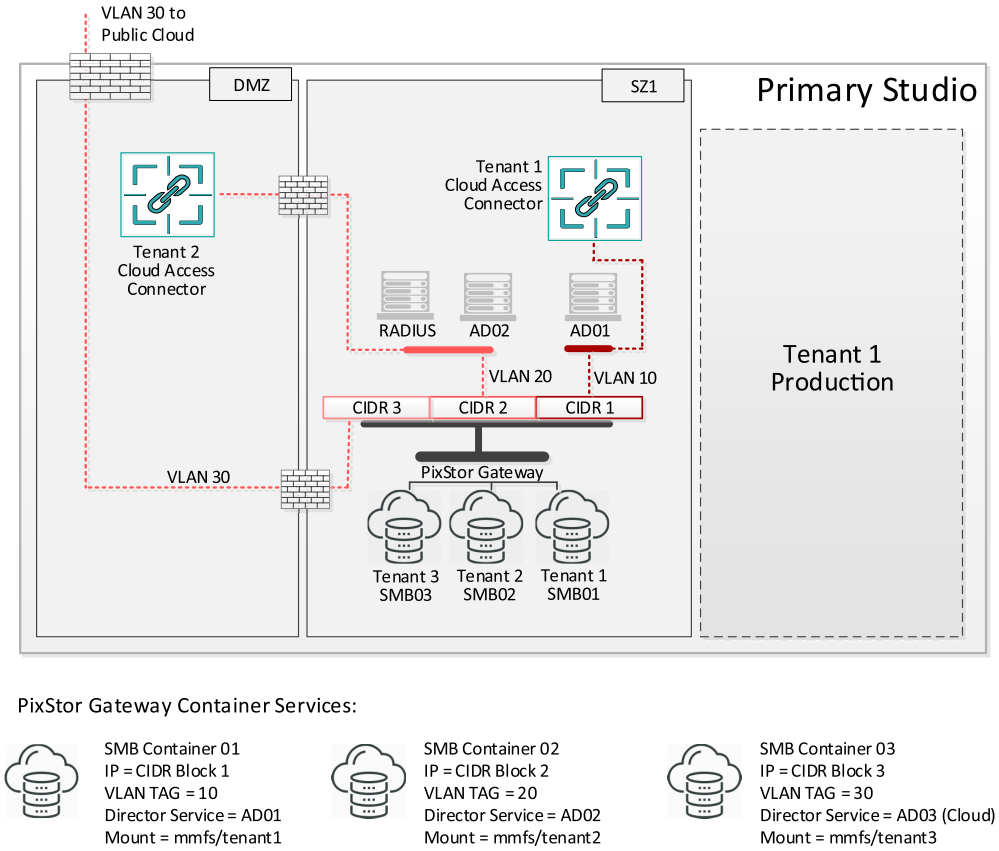
Artists require access to corporate desktops for office applications and public internet access which are isolated from the production network. Rather than equipping artists with deskside machines that compromise compliance, they are assigned a corporate desktop (typically a virtual machine) with Cloud Access Software in a separate corporate infrastructure security zone which enables a double-hop isolated PCoIP connection between artist and corporate facilities, including public internet access as illustrated below.



Corporate Infrastructure Isolation

PER-TENANT NETWORK AND STORAGE ISOLATION

The PixStor platform provides multi-tenant enterprise-class containerized NAB services enabling logical separation of data on a single storage fabric by only serving it out to isolated production networks. Referring to the illustration below, production networks are separated as Layer 2 VLANs, each served by a dedicated active directory. The template below has AD01 and AD02 located on-premises and AD03 located in the public cloud.



Network and Storage

Referring to the illustration, VLAN's 10, 20 and 30 supports tenant 1, 2 and 3 respectively. Classless Inter-Domain Routing (CIDR) separates storage at bit-level granularity with CIDR 1 thru 3 supporting respective VLANs. The VLANs are trunked back to the PixStor Gateway which fronts the back-end storage network. Networked file sharing is accomplished via SMB protocol (Simple Message Block), each tenant VLAN associated with a separate container, physical NIC affinity and mount as specified in Pixtor Gateway Container Services. Instead of attaching workstations to NAS Services in the PixStor head, the services are run inside a container cluster with a set of folders attached only to the tenant VLAN.

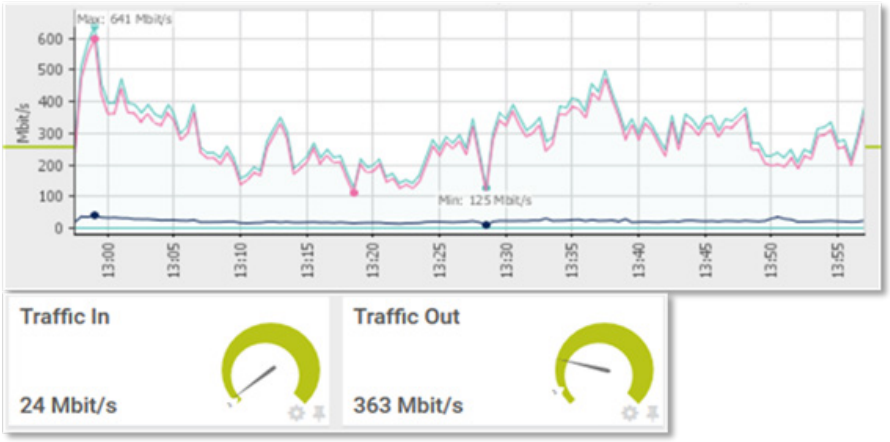
Performance Aspects

REMOTE WORKSTATION PROXIMITY

It is important that any virtual studio is location sufficiently nearby either the private data center or public cloud workstation resources to ensure satisfactory interactivity between artists and their creative software applications. If the round-trip time (RTT) latency becomes too high, interactive devices such as pen tablets feel heavy-handed which impedes productivity. For low-latency networks (i.e. less than approx. 10ms - 15ms RTT), the USB signals for peripheral devices such as tablets can be terminated at the remote workstation and remain highly responsive. For higher latency networks (approx. 15ms - 25ms RTT), Teradici provides 'local termination' of specialist USB devices such as WACOM tablets, both for software-based and Zero Client endpoints which expends the responsive operating range of the devices. Depending on the specific role of the artist, productivity diminishes over the 25ms – 50ms RTT range. The good news is that regional footprints of major CSPs are proliferating quickly which means many cities of the world are serviced by public cloud resources well within latency limits.

NETWORK CAPACITY PLANNING

Interactivity aside, each user should be assigned enough PCoIP network bandwidth to ensure uncompromised image quality and frame rate. While per-user peak bandwidth demand is highly variable and should be configured according to published PCoIP Session Planning guidelines, only changing pixel data is transmitted (i.e. a static desktop display consumes no bandwidth) which means average studio-wide consumption is a fraction of aggregated per-user peak demand.



Example: Studio-wide Network Bandwidth Consumption

The above infographic provides a real-world example of total network bandwidth consumption for a virtual studio of approximately 70 artists over a one-hour period – each artist has a Zero Client and dual 1920 x 1080 FHD displays. The total 'Traffic Out' network bandwidth of 363 Mbit/sec translates to an average per-artist bandwidth of less than 10 Mbit/sec. It is recommended that capacity planning be based on a real-world Proof-of-Concept or existing metrics for your own studios because exact network bandwidth is dependent on artist role, frame rate requirements, image quality and display topology.

CLOUD STORAGE CACHE INFRASTRUCTURE

The PixStor Cloud solution provides a full software-defined scale-out filesystem in the public cloud that can replicate on-premises storage, presenting an in-cloud 'local' NAS for public cloud remote workstations. PixStor Cloud enables a complete view of the on-premise storage to cloud workstations and automatically migrates data on access, which ensures that only requisite data is transferred by the public cloud. Data generated by the public cloud workstations can be migrated back to on-premise storage by PixStor as soon as written, letting artists continue work with minimal disruption.

PixStor Cloud also accelerates cloud-based rendering and overcomes complexities, transfer delays and cost overruns by seamlessly extending on-premises storage into the cloud which minimizes latency between where the data is stored and where it is processed, which ensures rapid completion times and low per-instance render costs.

Architecture Scalability

An essential attribute of this reference architecture lies in its ability to scale both individual virtual studios (i.e. additional users) and scalability of the overall architecture (i.e. additional virtual studios). The Teradici Cloud Access Manager is key to such scalability – it comprises two components, namely a Cloud Access Manger SaaS service (included with Cloud Access Software subscriptions) and the Cloud Access Connector component shown in the illustrations above which provides connectivity between PCoIP endpoint devices and remote workstations.

SCALING WITHIN A VIRTUAL STUDIO

Scaling a studio entails adding workstation resources, storage and network capacity to accommodate added users. From a workstation management perspective, public cloud workstation resources can be instantiated from the Cloud Access Manager Console using default or customized machine templates. If the remote workstations are located on-premises (e.g. HCI or VMware ESXi), they are added to the existing tenant deployment. New users in Active Directory are then assigned to remote workstations from the Console. Cloud Access Manager also includes power management resources to effectively manage up-time and related costs of public cloud workstations.

ADDING A VIRTUAL STUDIO

A new studio is deployed by assigning VLAN, Storage and Active Directory components and adding a new Cloud Access Connector to support brokering between new users and newly allocated remote workstations. A Cloud Access Connector can be deployed in any geographic region supported by the CSP so setting up an offshore studio involves instantiating workstation and storage resources within a Virtual Private Cloud in proximity to the physical location of the offshore studio, and then deploying a Cloud Access Connector to facilitate connection brokering.

About

Jellyfish Pictures

Jellyfish Pictures creates visual effects (VFX) and animation for advertising, film, and television. The company has won Emmy, VES, and BAFTA awards.

jellyfishpictures.co.uk

Pixit Media

Pixit Media develops data-aware, software defined infrastructure solutions for the Post-Production and Broadcast industries.

pixitmedia.com

Teradici

Teradici is the creator of PCoIP remoting protocol technology and Cloud Access Software. The company is focused on its core mission of seamless delivery of workstations and applications for end-users.

teradici.com