Pivot 3

Creating a Foundation for Safer, Smarter Airports

Sample Reference Architecture

Table of Contents

Introduction

Airports make up a vital component of any city's critical infrastructure with strong influences on the economy, tourism and the functioning of the city. Thus, as cities continue to get smarter as they move towards the future, it is imperative that airports follow suit. This must be tempered with the increased resilience and security that an airport requires to ensure non-disruptive operations and public safety. All of this relies on technology and building a solid, intelligent foundation on which to run that technology is now more important than ever before.

This Pivot3 Sample Architecture outlines some, but by no means all, of the requirements that an Airport Security Officer should consider when designing the infrastructure to run their airport security systems on. It then goes on to highlight some of the Pivot3 technologies that aid airports in achieving these goals. Finally, a composite airport infrastructure is presented, based on a number of existing Pivot3 airport installations and an infrastructure solution design is presented that is capable of delivering all of the benefits defined.

NOTE: The solution configuration and sizing calculations in this document are for illustrative purposes only and do not apply to any other workload type. The data represented here should be used as guidance only. Actual workload requirements will vary based on unique deployment characteristics and requirements. Consult your Pivot3 Solutions Architect for unique configuration and sizing requirements.

Understanding Airport Security Infrastructure Requirements

Airports are complex environments, which often leads to that same complexity being mirrored in the design of the security infrastructure. In this chapter, we are going to examine a number of the key requirements in designing a successful airport security infrastructure.

Capturing High Quality Video

Incident management relies on clear, crisp video imagery being captured, whether it is to identify persons of interest, capture the small details vital in giving the full context to a situation or using video as a source for analytics software. While cameras have evolved rapidly over the last 25 years, from VGA to 4K and even 8K in some cases, the infrastructure that is recorded the video has often struggled to keep up.

When you ally the increased requirements of capturing 30FPS (Frames Per Second) with the increased frame sizes that higher resolutions cameras deliver, you have a choice to make. You can either reduce the number of cameras per NVR or SAN Controller and increase the amount of cost, complexity and management overhead; or you can look at a solution that was designed specifically for video surveillance environments, which takes advantages of modern technologies to ensure video is captured without dropping a frame, but remains flexible and scalable to grow and adapt as your requirements change.

Delivering A Zero Downtime Infrastructure

Airports are 24/7 operations, regardless of whether planes are landing or not and it is imperative that the physical security infrastructure remains operational at all times, making hardware and software resilience a necessity. The majority of infrastructure options will deliver a degree of resilience, whether it is using a RAID5 data protection scheme to protect against a single drive failure in an NVR (Network Video Recorder) or using dual-streaming from a camera to 2 separate SANs (Storage Area Network) to ensure that video is still being captured in event of a full SAN failure.

What is less often considered is the impact of that failure on the video being captured, and the accessibility of the video that has been captured already. Failures in security infrastructure can cause wider disruption to the terminal, and in the case of missed incidents, liability can fall on the airport operator. With that in mind, it should always be the case that your physical security infrastructure still captures video without frame loss during degraded operations and that your video still be accessible during those failures.

It transpires that the ability to deliver this on a traditional IT infrastructure is expensive and limited, usually resulting in the duplication of expensive SAN hardware, alongside licenses for replication technologies, in a centralized storage model, or the doubling of the number of NVRs that you have in the environment, and the cost of adding a dual streaming license to each camera for a NVR type design, increasing the management and maintenance of the infrastructure.

One of the core principles of any physical security infrastructure design should be the combination of resilience in a minimized footprint.

Meeting Data Storage Requirements

With the increases in video quality and a hike in the number of cameras being deployed throughout critical airport infrastructures, the storage requirements for that video, along with retention periods and data protection for that video have increased dramatically. It is certainly not uncommon to see multi-petabyte (PB) deployments in a large number of Pivot3's airport installations.

With these increases, the cost of that storage is also increasing, making storage efficiency and data protection important factors to consider in any design. Using traditional datacenter technologies for data protection, like snapshots, replication and backups are often impossible to achieve technically, and cost prohibitive even if they can be done. Losing security data, especially video, can lead to liability implications if an incident is missed as a result. Often, realization that video is of insufficient quality, or missing altogether occurs after an incident when the footage is under review.

New methods of data protection and a storage efficiency that can comfortably manage multiple petabytes of data should be an integral part of your infrastructure design.

Managing A Distributed Infrastructure

Airports are large sites, commonly having security infrastructure in a number of locations for either performance or technical reasons and often for the convenience to the users. Managing this type of distributed infrastructure on an individual basis can present a number of challenges, most critical of which is the constant monitoring and resolution of any hardware or software failures. It is also common to have duplicate infrastructure based on the requirements of the different agencies involved with the airport, for data security or operational needs, however the management of all of this infrastructure commonly falls to the security team, or the IT department.

When centralization of the infrastructure isn't possible, it is vital to have a centralized management and monitoring of the infrastructure that you have distributed. Hardware failures and performance problems can be resolved more quickly, and the auditing and reporting of the infrastructure is made simpler.

Enabing Multi-Agency & Multi-Tenant Collaboration

As we just mentioned, there are multiple agencies and tenants that have an operational requirement based in the security team and each agency has their own preferences, operational models and requirements for data management and data security. This has previously led to duplicate hardware and increased cost of deployment and ongoing management for the airport security team.

It's not just the federal agencies that an airport has to work with and deliver infrastructure for. Commonly, the airlines themselves have a requirement for security services and increasingly, are looking for data services to help them improve their passenger experience and service.

Being able to create a cryptologically unique and secure environment is a real possibility for these multi-agency environments and can be used to drive an improved level of standardization, operational cost reduction and simplification of the infrastructure.

Running Multiple Applications & The Increased Adoption Of Virtualisation & Analytics

Physical security has a lot to gain from deploying their infrastructure on a virtualized platform. Most notably, the increased tolerance to hardware and software failures where applications can move seamlessly between servers to ensure the constant operation of the airport security infrastructure.

Further to this, there is an opportunity for consolidation of those applications onto a single platform, especially compared to traditional solutions, where the deployment of each new security applications or video analytics leads to the additional hardware costs being incurred. As long as the environment is sized appropriately, then it is possible to run security applications on the same hardware as the video surveillance infrastructure, reducing hardware costs, increasing resilience and improving the performance of the infrastructure as a whole. This must also be achieved without compromising on the security of the infrastructure.

With virtualization being a core datacenter practice, it is also beneficial should the IT department be responsible for the management of the security infrastructure hardware components since a virtualized platform will fit in with their current management practices and procedures.

From Security To Business Value & Moving Beyond Video

Increasingly, video surveillance and security applications are being asked to aid the business in driving "value", without compromising the security function it was originally designed to provide. This is because video is an incredibly rich source of information that can be used to improve client engagement or deliver data to non-security stakeholders designed to improve their sales and customer service.

This request should not be discarded, as if done correctly, benefits can be applied to the security team, with many of the analytics packages and opportunities also able to deliver increased security benefits and in some situations, allowing the security team in some Pivot3 customers to move from being a cost center to being cost neutral, or even becoming a profit center.

The type of data collected isn't solely video related; mobile device tracking has proven to be an incredibly valuable and useful source of information, especially in situations where video is less valuable (facial obscuration, incomplete video files, poor video quality, asset tracking etc).

Pivot3 Hyperconverged Infrastructure Architecture

In the previous section, we looked at some of the challenges when designing an airport infrastructure and how the myriad requirements that every security officer at an airport must consider can lead to design complexity and an inefficient system that doesn't always represent good value for money, nor meet all of the security requirements in a comprehensive manner.

In this section, we will examine some of the technologies and features employed by Pivot3 to simplify this complex design into a modular, scalable, flexible and secure platform that will comprehensively meet the needs of the airport now and as it continues to evolve.

More technical information can be found in the Pivot3 Surveillance Series Whitepaper, available *here*.

Hyperconverged Infrastructure (HCI) Overview

HCI hit the mainstream in 2009 and is fast becoming the infrastructure platform of choice throughout the datacenter market. The concept of HCI brings together the storage, compute and networking aspects of IT hardware and combines them into a single, modular infrastructure that increases the flexibility, scale and performance of an environment by using commodity, off-the-shelf hardware. More information on the core concepts of HCI may be found *here*.

Pivot3 HCI was designed specifically for video surveillance and security, using a large number of patented technologies, alongside the industry leading virtualization platform, VMware ESXi, to create a secure, resilient and flexible solution that offers simple management at scale from a centralized location.

Simply put, Pivot3 drives a more cost-effective and efficient infrastructure for airports. The proof is evident in the large number of regional, national and international airports that have deployed Pivot3 across the globe.

Capturing Video Without Frame Loss

Industry tests have demonstrated that video surveillance performance is predicated by the amount of throughput available and the number of drives available to write the data to. These figures directly influence the number of cameras (depending on frame rate, compression codec and resolution) that may record to a specific device or storage volume. If this is mis-calculated, or the parameters being recorded change, then video quality may suffer, or additional hardware may have to be deployed, alongside a painful rebalancing of cameras.

Pivot3 aggregates all of the drives across all of the nodes in the cluster to create a single pool of storage that can be flexibly assigned to the Video Management Server (VMS) and also deliver a much greater amount of overall bandwidth to the cameras to record to. The net benefit of this is a reduced footprint for the hardware, and a greater cameras density per node, helping to reduce cost and management overhead.

This approach also ensures that video is captured without the possibility of losing frames, even in a degraded state.

Protect Against Hardware & Software Failure

As airports are reliant on security to ensure operational success, ensuring that the hardware and software they use remains running is critical. Pivot3 provides a number of features to ensure that the security infrastructure is kept operational at all times.

Erasure Coding Data Protection

Pivot3 uses a proven technology called Erasure Coding to protect the data being written to the infrastructure. This has a number of benefits over the traditional data technologies (RAID and Replication for example) used both in video surveillance and datacenter environments and is used by the likes of Google, Amazon and IBM to protect large volumes of data.

By using Erasure Coding, Pivot3 is able to protect for up to 5 simultaneous drive failures in a single cluster, or an entire node and 2 additional drives simultaneously without losing service or compromising on video quality. This level of protection is also achieved with a higher level of storage efficiency than traditional RAID or replication technologies.

Pivot3 Failover

There are 2 options for managing entire node failure within Pivot3, depending on what version of virtualization you are using. If you IT team has deployed VMware ESXi and is responsible for the management of the infrastructure, then Pivot3 is able to integrate seamlessly and take advantage of the inbuilt failover technologies. If this is the first virtualized environment that's being deployed by the airport, Pivot3 uses an inbuilt failover technology to reduce the license costs for virtualization but provides the same level of protection and failover capabilities.

Both of these failover technologies are automated and designed to ensure that there is no disruption to the environment and downtime is mitigated.

Proactive Monitoring

It is a known fact that failures will occur, both in hardware and software, so the ability to proactively monitor and deliver a faster resolution to the failure limits the amount of disruption and downtime that the environment may experience.

Pivot3 proactively monitors and reports on the health of the Pivot3 infrastructure to ensure that your system administrators are always aware of the health and status of this critical airport infrastructure. With this proactive monitoring being delivered via a centralized management interface, the location of the hardware becomes less important and distributed architecture limitations can be removed.

Quick Node Rebuild

One of the primary challenges associated with RAID technologies as drive capacities have increased is the amount of time that the system takes to recover from a failure. In large capacity hard drives, using RAID5 or RAID6, the recovery from a drive failure can take hundreds of hours, leaving your infrastructure in both a vulnerable state and impacting performance, which may lead to video loss, or a reduction in video quality, which in turn may cause an incident to be missed, or your analytics platform to perform less than optimally. This is unacceptable in all scenarios.

Pivot3 has implemented a technology called Quick Node Rebuild, which enables the recovery for an entire node failure to be completed in less that 1/10th of the time it can take a RAID based infrastructure to recover from a failure. This ensures that the airport infrastructure is back to optimal performance and protection more rapidly and reduces the risk of multiple failures leading to data loss.

Scalable, Flexible Infrastructure Growth

By employing a modular design, Pivot3 airport customers are empowered to make their own choices when it comes to deploying their infrastructure and managing it, meeting their requirements more effectively than outdated traditional designs.

In a distributed architecture, differing sizes of node may be deployed to ensure that there isn't wasted resources in those locations, and each cluster can be scaled independently as that section of the environment scales. By being able to do this non-disruptively and flexibly, unforeseen requirements (changes in compliance or retention) can be met agilely, and future projects can be deployed as necessary, without an expensive hardware infrastructure purchase being associated with it.

For a centralized infrastructure, airport security directors inform us that the ability to add nodes as the various phases of the project take place has enabled them to budget more efficiently and also scale flexibly as plans and requirements change. With this in mind, it is no surprise that 70% of Pivot3 airport installations[1] have deployed further nodes as part of planned infrastructure expansions within a year of their first deployment.

This approach to delivering new services allows a security team to take advantage of new technologies and have them operational more quickly, improving the levels of service and security they are able to provide.

Centralized Management

Depending on the size of the airport customer and the operational requirements that customer has in terms of hardware separation and localization it is very easy for security infrastructure to become distributed throughout the entire airport site and increase management overhead dramatically.

[1] Correct as of December 2018

Regardless of which architecture our customers choose, Pivot3 nodes are managed centrally giving you direct access to the hardware status, consoles and with the ability to make changes on the fly from one management interface.

For those customers who are familiar with virtualization, or have the IT department managing the security infrastructure, Pivot3 is deployed as a plugin within the vCenter management console, bringing additional benefits to systems administrators around maintaining current management policies and strategies, as well as giving a single point of reporting for all audit and compliance requirements around system infrastructure and management.

Secure Multi-Tenancy Options

Airports are complex environments in normal situations, but when you add the multi-agency and multi-tenant collaboration requirements, it can soon scale out of hand, especially if each agency is looking for a specific set of requirements. This can very quickly lead to sprawling infrastructures with a large amount of duplication and additional cost. In some scenarios, Pivot3 has seen each agency and airline deploy its own dedicated infrastructure, VMS and applications to deliver the same functions, increasing the operational costs and management exponentially within the airport.

Pivot3 has a series of data security features described in more detail *here* that can enable a customer to deploy a secure, multi-tenanted infrastructure where each agency can conform to its own regulations and requirements, but without dramatically increasing the cost of hardware.

Each storage volume is cryptologically unique, with its own set of encryption keys, access control features and authentication practices. It can be forensically audited and has been proven to meet a number of Federal data management regulations and statutes.

By reducing the hardware footprint but maintaining the flexibility of the solution to scale on demand to meet any new needs an agency requests, airports can deliver an agile “service-like” infrastructure, without increasing hardware footprint and management overhead.

Multi-Application Infrastructure & Analytics Integration

Security cannot just be considered as video surveillance; access control, VIP management, wayfinding, restricted areas and VIP management form a large part of an airport’s security strategy. In traditional solutions, each application would require dedicated hardware, which increases the cost of the solution dramatically. By using a virtualized infrastructure, Pivot3 allows for multiple security applications to be deployed on a single platform, reducing the footprint and cost of the solution, but also providing a readily available platform to deploy new technologies to, improving the time in which it takes an application to be production ready.

By using a modular infrastructure, expansion of the infrastructure is simple and non-disruptive, creating a more agile airport security team, able to deploy and have security application operational in a shorter time, without incurring the cost and deployment and interoperability pain of stand-alone solutions.

Pivot3 partners with the leading analytics companies, creating an array of validated solutions covering a host of security applications. This program includes NVIDIA and the GPU cards that many analytics applications rely on for performance and processing data.

Many airports are now consolidating IT applications and security applications onto a shared infrastructure to reduce costs and complexity, and Pivot3 have a range of datacenter solutions to enable this to happen, providing all of the benefits outlined in this paper to the datacenter, and non-security aspects of the airport infrastructure. More information on how we helped an international airport on the East Coast of the USA achieve this can be found *here*.

Sample Design

Having understood some of the challenges and their potential solutions, we move into an examination of a design for an airport security infrastructure. We referenced a number of Pivot3 airport customers and the associated RFI (Requests for Information) documents and RFP (Requests for Proposals) documents and created a composite airport customer.

Composite Organization Details

Camera Information

The airport in this scenario has laid out the following video camera requirements; The composite airport has chosen to run the Milestone xProtect Corporate Edition as the VMS for the solution, citing its open platform design making it perfect for future expansion and integration of analytics packages.

There is currently no firm requirement for the airport to capture, manage and provide video surveillance services for the airlines or other agencies within the airport, although there is a future planned "consolidation and co-operation" drive, with a secure, multi-tenanted environment being the desired outcome.

Camera Count	Camera Resolution	Recording Details	Camera Use
400x	1600x1200 (2MP)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	Fixed Camera at 2MP
80x	2560x1920 (5MP)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	Fixed Camera at 5MP
1000x	1280x1024 (1.3MP)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	PTZ Camera at 1.3MP
50x	3840x2160 (4K)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	Multi-Sensor Camera at 8MP

150x	2944x2208 (9MP 360 Deg)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	360 Degree Camera at 9MP
320x	2288x1712 (4MP)	H.264-Good, 75% Motion, 30FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	Fixed Camera at 4MP
500x	1280x1024 (1.3MP)	H.264-Good, 75% Motion, 15FPS), 30 Days Live, 60 Days @ 4FPS, 100% Recording)	Fixed Camera at 1.3MP

Additional Applications

There's also a requirement from the airport for the following applications, to be incorporated into the infrastructure design under a single management interface with hardware standardization and GPU integration where possible.

Design Tools & Calculations

In order to generate an accurate calculation of the necessary bandwidth and storage capacities required, we used a readily available, industry approved tool, JVSG (*www.jvsg.com*). The calculations are summarized in the table below.

Resolution	Compression	Image Complexity	Motion %	Frame Size*, KB	FPS	Days	Camer...	Recording %	Bandwidth, Mbit/s	Disk Space, GB	Bitrate,kbit/s	Co
1600x1200 (2 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	22	30	30	400	100	2162.69	700710.9	5407	
1600x1200 (2 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	34	4	60	400	100	445.64	288777.8	1114	
2560x1920 (5 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	55	30	30	80	100	1081.34	350355.5	13517	
2560x1920 (5 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	88	4	60	80	100	230.69	149485	2884	
1280x1024 (1.3 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	15	30	30	1000	100	3686.4	1194393.6	3686	
1280x1024 (1.3 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	23	4	60	1000	100	753.66	488374.3	754	
3840x2160 (8 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	94	30	30	50	100	1155.07	374243.3	23101	
3840x2160 (8 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	148	4	60	50	100	242.48	157129.1	4850	
2944x2208 (9mp 360)	H.264-30 (Average Quality)	50 - Average	80 - Active	73	30	30	150	100	2691.07	871907.3	17940	
2944x2208 (9mp 360)	H.264-30 (Average Quality)	50 - Average	80 - Active	116	4	60	150	100	570.16	369465.8	3801	
2288x1712 (4 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	44	30	30	320	100	3460.3	1121137.5	10813	
2288x1712 (4 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	70	4	60	320	100	734	475634.1	2294	
1280x1024 (1.3 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	15	30	30	500	100	1843.2	597196.8	3686	
1280x1024 (1.3 MP)	H.264-30 (Average Quality)	50 - Average	80 - Active	23	4	60	500	100	376.83	244187.1	754	

Each camera has been broken down into the "live" 30-day recording requirement at 30FPS and the subsequent 60-day "archive" period at 4FPS.

The total bandwidth and storage capacities required are 19.5Gbits/s and 7.3PB of storage. Once we further calculate a 20% overhead in accordance with Pivot3 best practices to ensure smooth playback, and as a buffer for more complex scenes, incident storage and changes in motion, we arrive at figures of 22.5Gbit/s and 8.8PB of storage.

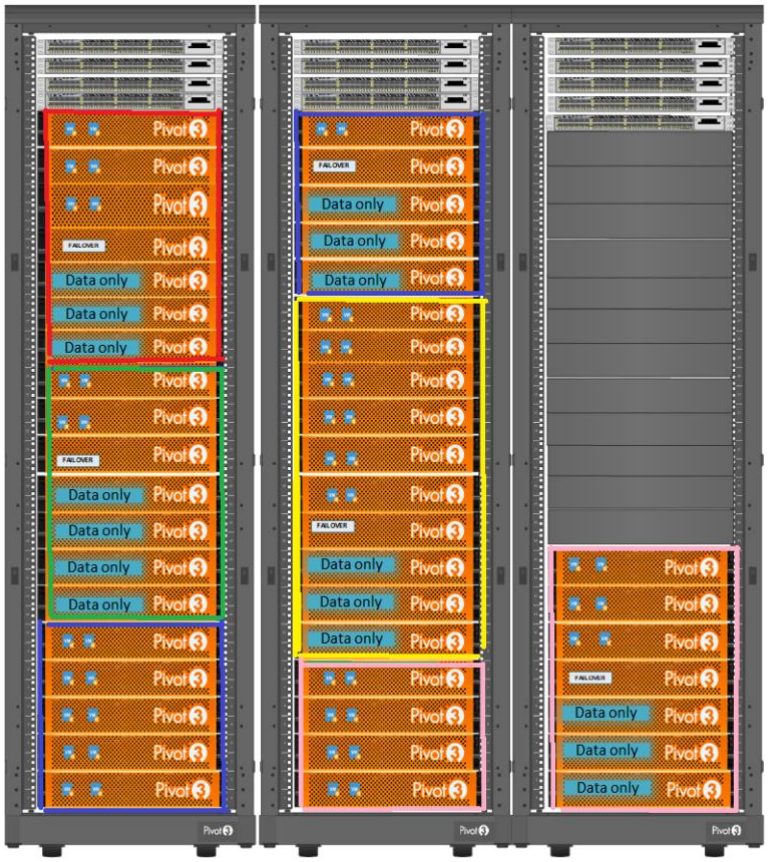
Total FPS	Disk space,GB	Bandwidth, Mbit/s
85000	7382998.1	19433.53

Pivot3 Sample Design

The Pivot3 diagram below provides the required storage, bandwidth and processing power to deliver a fully functioning hyperconverged solution for the airport to capture 2500 cameras with a variety of recording rates, resolutions and mixed requirements.

The immediately obvious benefit is that 10.1PB of storage is contained in less than 3 racks of infrastructure and incorporates the compute, storage and networking required to meet the airport requirements completely. The consolidation of hardware in this way presents a large cost saving in datacenter power and cooling expense and provides assistance in meeting the environmental targets currently being set within the airport industry.

Pivot3 has a unique ability to scale the infrastructure in future node-by-node, and with scaling able to take the form of a “full” HCI node with both storage and compute; a “data only” node, which has additional capacity without the cost of a compute platform, but still adds cumulatively to the performance of the vPG; or a “Compute” node, which delivers a high performance compute layer, ideal for advanced analytics, dense GPU deployments and applications when the airport doesn’t require additional storage.



Broken down into 5 virtual Performance Groups (vPGs, essentially a cluster) to meet the requirements of the airport. The table below illustrates the configuration of the nodes used and provides the function of the vPG as part of the wider solution.

VPG (Outline Colour)	V5-2000s Surveillance Nodes	V5-2000s Storage Nodes	No of CPU Cores	Total Memory Per Node	VMS Recording Servers Per Node (Total)	Useable Storage (TB)	Total Bandwidth Per vPG (Mbit/s) (# Recording Servers)
Red	4	3	20	96GB	2 (6)	1,518TB	2500 Mbit/s (4) 1 Mgmt Server, 1 x Event Server
Green	3	4	20	96GB	2 (4)	1,518TB	2500 Mbit/s (4)
Blue	7	3	20	96GB	2 (12)	2,289TB	7500 Mbit/s (12)
Yellow	7	3	20	96GB	2 (12)	2,289TB	7500 Mbit/s (12)
Pink	8	3	20	96GB	2 (14)	2,803TB	7500 Mbit/s (12) 1 x Mgmt Server, 1 x Event Server
Total	**29**	**16**			**48**	**10,417TB**	**27,500 Mbit/s**

The Red and the Green vPGs are used for the “archive recording” aspect of the solution and are made up of the Pivot3 V5-2000-Large Scale Surveillance Appliances, the specifications for which is included below.

2U Surveillance – Large-Scale	2U Surveillance	1U Surveillance	2U Storage-only	2U Virtual Security
				
Model Name				
V5-2000	V5-2000	Edge Protect	V5-2000s	V5-6400
HDD Capacity (TB)				
S2: 192, 240, 288	**L2:** 12, 24, 48, 96, 120, 144 **D2:** 16, 32, 64, 128, 160, 192	4, 8, 16, 32	**S2:** 192, 240, 288 **L2:** 12, 24, 48, 96, 120, 144 **D2:** 16, 32, 64, 128, 160, 192	-
SSD Capacity (TB)				
-	-	-	-	3.8
SSD Caching				
Yes	Yes	No	Yes	No
Max Appliances per vPG*				
12	12	6	12	16
Max Storage per vPG				
3.45 PB	2.3 PB	192 TB	2.3 PB	60.8 TB
Server Virtualization				
VMware Foundation	VMware Foundation	VMware Foundation	-	VMware ESXi
Virtual Clients				
-	-	-	-	VMware Horizon
Software Defined SAN				
Yes	Yes	Yes	Yes	Yes
GPU				
-	-	-	-	1-2x NVIDIA Tesla M10 or M60
PCoIP Offload				
-	-	-	-	1x Teradici Apex 2800 LP
CPU				
2x 12 Core Intel 4116 or 2x 20 Core Intel 6138	1x 12 Core Intel 4116 or 2x 12 Core Intel 4116	1x 4 Core Intel ES-1270	**L2 & D2:** 1x 6 Core Intel 3104 **S2:** 2x 6 Core Intel 3104	2x 20 Core Intel 6138
RAM (GB)				
64, 96	48, 96	16, 32, 64	32	384, 768, 1536
Networking				
6x 10GbE (SFP+ or RJ45)	6x 10GbE (SFP+ or RJ45)	4x 1GbE (RJ45)	4x 10GbE (SFP+ or RJ45)	6x 10GbE (SFP+ or RJ45)

** A Virtual Performance Group (vPG) is a logical, scale-out construct that includes both virtualized servers and storage.*

Each vPG also includes a dedicated failover node to ensure that the system remains operational and video is captured without frame loss even during full node failures. Each vPG delivers 2500Mbit/s of bandwidth, comfortable exceeding the 2173Mbit/s required for the archiving part of the solution. Both vPGs also take advantage of the Pivot3 "data" node, which is a fully functioning node for storage, bandwidth and resilience, but lacks the compute platform and hypervisors found in a "full" node. This saves the airport several thousand dollars per node in hypervisor licensing without sacrificing performance or resilience. Pivot3 is unique in having this solution.

The Red vPG also runs a management server and an event server for the Milestone VMS.

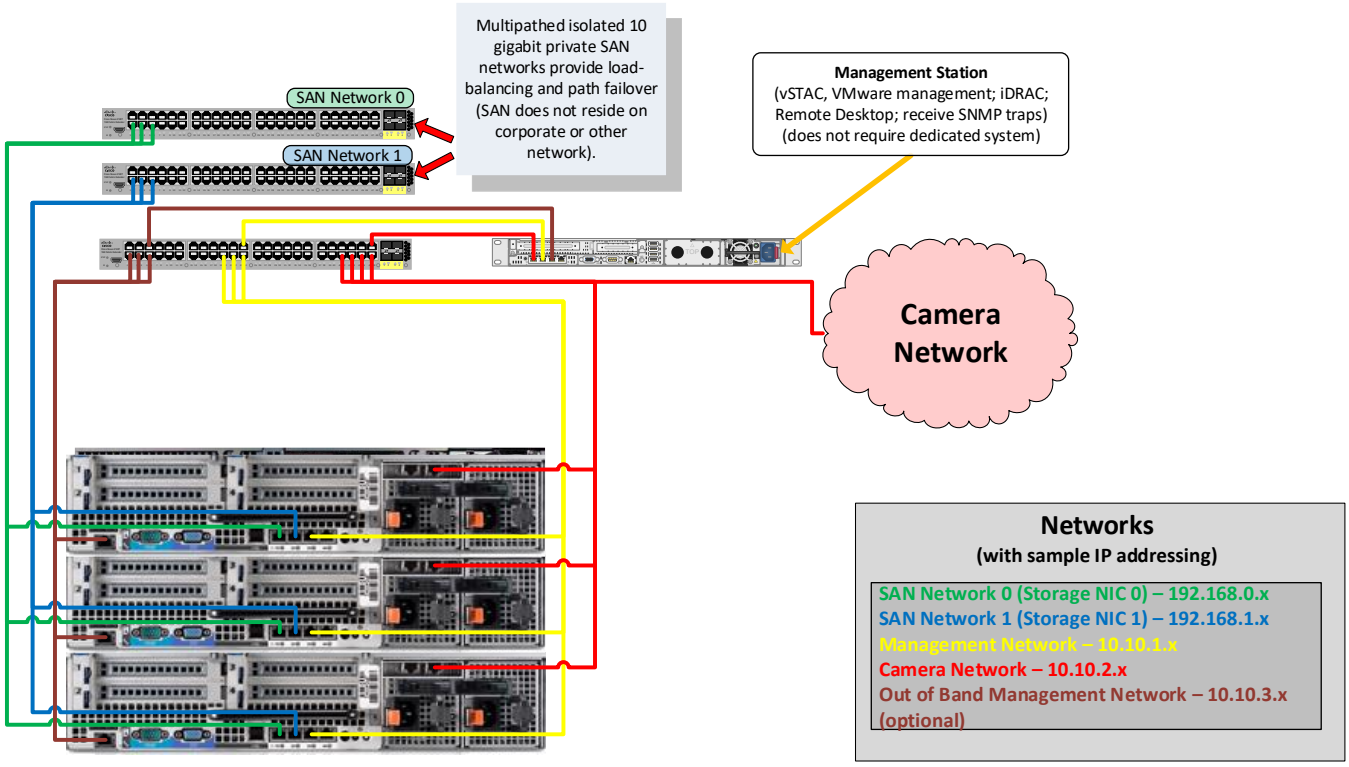
The remaining vPGs (Blue, Yellow and Pink) are all dedicated to the capture of the live video data, with the usual high frame rates and video quality associated with an airport.

The Blue and Yellow vPGs are made up of 7x V5-2000-large-scale nodes and 3x V5-2000s data nodes, as previously outlined in the datasheet table, providing the compute platform for 12 video recording servers with a dedicated

failover node to offer the required system resilience. Each vPG deliver 7500Mbit/s of throughput and a total usable capacity of 2289TB or 2.235PB.

The Pink vPG is similar to the Blue and Yellow vPGs with the exception of an additional V5-2000s node in order to provide a redundant management and event server for the Milestone VMS.

Pivot3 also delivers multiple layers of resilience within the networking, as the sample wiring diagram below illustrates.



Conclusion

The Pivot3 hyperconverged airport infrastructure in this sample architecture delivers a total of 27,500Mbit/s and 10.17PB of available storage. This will deliver exemplary performance to the airport allowing for high quality video capture, without frame loss, as well as a smooth playback of multiple cameras simultaneously. The failover nodes and redundant management and event servers deliver the expected levels of resilience to ensure that the airport remains operational, even during multiple hardware failures.

With the additional storage available and modular infrastructure, it would be simple for the airport to scale the solution to create a multi-tenant infrastructure to offer video surveillance and analytics services to the airlines and additional government agencies with security interests in the airports. The modular nature of the solution would also allow for that integration to take place at a pace and time to suit the airport without having to make additional infrastructure investments up front. The virtualized nature of the solution also allows for multiple different VMS, analytics, and other security applications to be deployed without conflict.

Overall, Pivot3 represents the most resilient, efficient and scalable infrastructure available to deliver the security and services required to enable your safe, smart airport.

Appendices