Dell Technologies IoT Solution | Surveillance with Genetec Security Center

Surveillance

December 2018

H17435

Configuration Best Practices

Abstract

This guide is intended for internal Dell Technologies personnel and qualified Dell Technologies and Genetec partners. It provides best practices for configuring the Dell Technolgies IoT Solution | Surveillance with Genetec Security Center 5.7 video management software.

Surveillance Lab
Validated

Published November 2018

Dell believes the information in this publication is accurate as of its publication date. The information is subject to change without notice.

THE INFORMATION IN THIS PUBLICATION IS PROVIDED “AS-IS.“ DELL MAKES NO REPRESENTATIONS OR WARRANTIES OF ANY KIND WITH RESPECT TO THE INFORMATION IN THIS PUBLICATION, AND SPECIFICALLY DISCLAIMS IMPLIED WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. USE, COPYING, AND DISTRIBUTION OF ANY DELL SOFTWARE DESCRIBED IN THIS PUBLICATION REQUIRES AN APPLICABLE SOFTWARE LICENSE.

Dell EMC
Hopkinton, Massachusetts 01748-9103
1-508-435-1000 In North America 1-866-464-7381
www.DellEMC.com

CONTENTS

CHAPTER 1

Introduction

This chapter presents the following topics:

Purpose

This configuration best practices guide aims to help Dell EMC field personnel understand how to configure the Dell Technologies IoT Solution | Surveillance with Genetec Security Center. This document is not a replacement for the Genetec implementation guide nor is it a replacement for the *Dell Technologies IoT Solution | Surveillance with Genetec Security Center Sizing Guide*.

In addition, this configuration guide describes how to configure VMware's Internet of Things (IoT) center. VMware IoT center provides an enterprise level IoT solution that uses cloud technology to simplify IoT device management.

The solution provides secure surveillance for the implementation of Genetec Security Center.

IoT Surveillance offers several key benefits including:

- Deployment and management
- Designed-In Security
- Scalability
- Tested and preintegrated solutions
- VMware vSAN provides:
  - Guaranteed high availability
  - Hyper-converged infrastructure (HCI) engineered for surveillance

Scope

This guide is intended for internal Dell EMC personnel and qualified Dell EMC and Genetec partners. It provides configuration instructions for installing the Genetec Security Center video management software using Dell EMC storage platforms.

The following VMware and Dell EMC storage systems have been tested:

- VMware vSAN
- Dell EMC ECS Object Storage

This guide supplements the standard and provides configuration information specific to Genetec Security Center.

Note

All performance data in this guide was obtained in a rigorously controlled environment. Performance varies depending on the specific hardware and software used.

Assumptions

This solution assumes that internal Dell EMC personnel and qualified Dell EMC partners are using this guide with an established architecture.

This guide assumes that the Dell EMC partners who intend to deploy this solution are:

- Associated with product implementation
- Genetec-certified to install Genetec Security Center services
- Proficient in installing and configuring ECS storage solutions

- Proficient in configuring VMware Software including vSAN and Pulse IoT center
- Familiar with installing and configuring VMware hypervisors and the appropriate operating system, such as Microsoft Windows or a Linux distribution

The configurations that are documented in this guide are based on tests that we conducted in the Dell EMC Surveillance Lab using worst-case scenarios to establish a performance baseline. Lab results might differ from individual production implementations.

CHAPTER 2

Configuring the Dell EMC solution

This chapter presents the following topics:

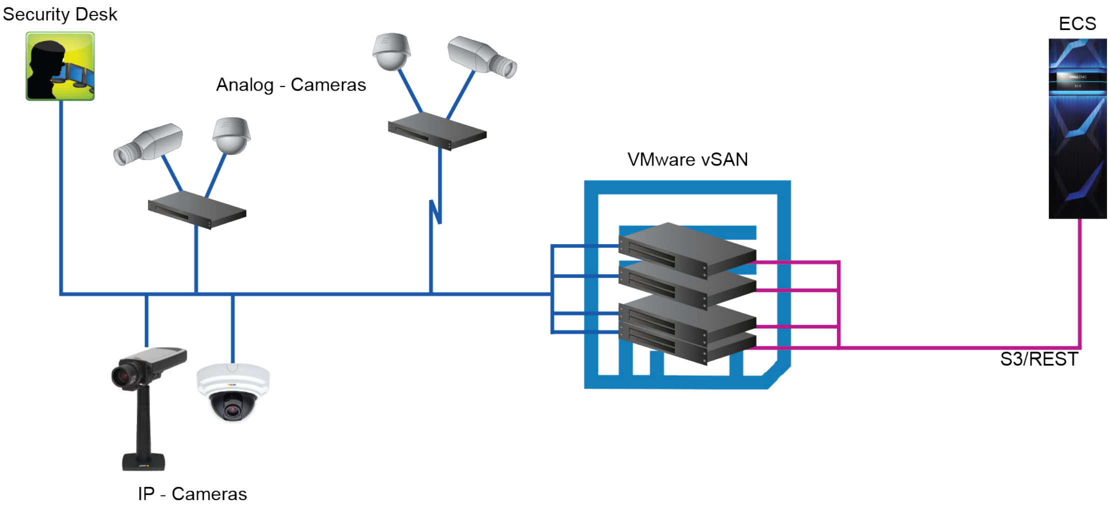
Design concepts and disclaimers

There are many design options for a Genetec Security Center implementation including Federations, Auxiliary Servers, and multicast considerations.

Genetec offers many courses that are related to design and implementation for those who require this information. These details are beyond the scope of this paper.

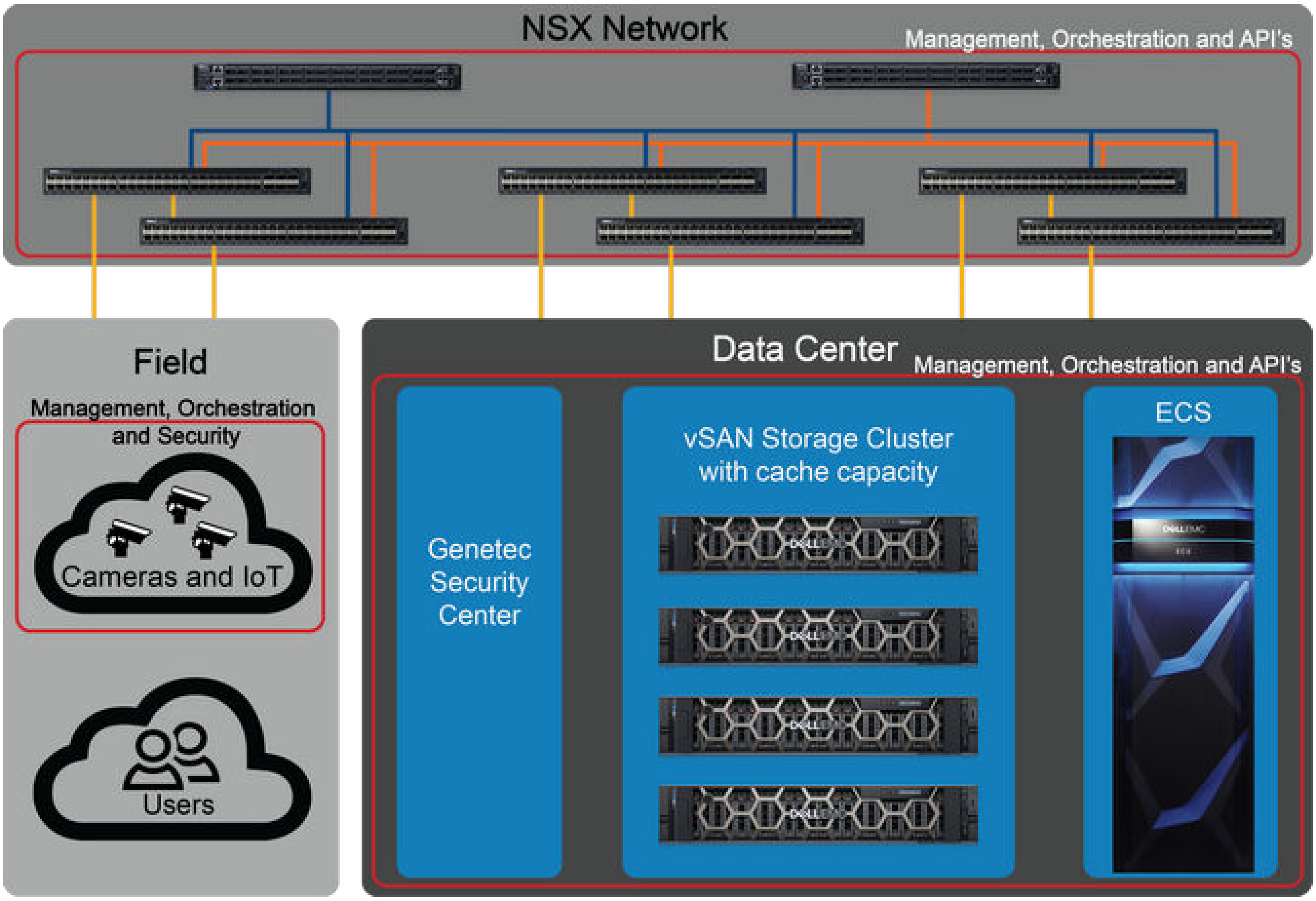
The following diagram illustrates the Dell EMC and VMware components that were tested.

Figure 1 Dell Technologies IoT Solution | Surveillance with Genetec Security Center architecture



The Dell EMC Surveillance Lab vSAN test environment uses various servers and storage options throughout the lab, as shown in the following figure. When conducting a test, the nodes are contained in a single cabinet. Traffic can originate from application servers within the cabinet or servers external to the cabinet or both. Any non-vSAN storage is external to the cabinet, which includes the ECS.

Figure 2 Dell EMC Surveillance Lab vSAN test environment


NSX Network
Management, Orchestration and API's
Field
Management, Orchestration and Security
Cameras and IoT
Users
Data Center
Management, Orchestration and API's
Genetec Security Center
vSAN Storage Cluster with cache capacity
ECS

The VMware software solution in this IoT surveillance environment uses VMware's Pulse IoT, vSAN, vSphere, and vCenter for IoT surveillance management. The vCenter Server provides a platform for managing vSphere while vSAN provides a scalable storage solution with high availability.

Dell EMC IoT Solution | Surveillance environment

The Dell EMC Surveillance Lab recommends the following base configuration for a successful implementation:

Virtualized environment

- 8 vCPUs
- 16 GB memory
- Network adapter type: VMXNET3 (GbE and 10 GbE)

R740xd vSAN Ready node (vSAN certified storage)

- Dual Intel Xeon gold 6126 2.6G, 12C/24T
- 192 GB memory
- 10x 3.84 TB SSD SAS Read Intense
- 2x 800 GB SSD SAS Write Intense

- Intel X710 Quad Port 10 Gb DA/SFP+ Ethernet, Network Daughter Card

vSAN cluster

- 4 R740xd vSAN Ready nodes
- 40 total capacity drives
- 8 Disk Groups (1 vSAN cache to 5 capacity SSD_
- 10 GbE NIC connections for:
    - vSAN
    - Administration
    - vMotion
    - vSAN Managment

Management cluster

- 4 R440 vSAN Ready nodes
- 128 GB memory
- 5 1.92 TB cluster drives
    - 1 flash cache drive
    - 4 storage drives

Switching

- Dual DellS4048s (leaf) vSAN cabinet: vSAN, vMotion, Camera/User
- DualDell Z9100s network core (spine) - optional

External storage

- ECS U4000
- 8 node with 60 drives per node

Supporting Servers

- Review stations: Dell PowerEdge servers - various models
- Work stations: Dell Precision - various models

Refer to the following network and design guides for more information on configuring vSAN for your environment, or contact ProDeploy Plus for vSAN configuration assistance:

- VMware Storage and Availability Technical Documents
- VMware vSAN Design and Sizing Guide
- VMware vSAN Network Design

All storage and server tests are conducted using 10 GbE NICs unless otherwise noted.

For all the tests, the virtual CPU (vCPU), memory, and network were configured according to Genetec best practices. The VMware vSphere configuration was in accordance with the VMware Compatibility Guide (www.vmware.com/resources/compatibility/search.php).

The Dell EMC Surveillance Lab's host hardware met and exceeded the minimum system requirements for an ESXi/ESX installation. The Genetec Archiver VM was running on an ESXi 6.5 host using Dell EMC PowerEdge 740xd Ready Nodes.

Releases validated

The following tables list the firmware builds and software releases used for our tests.

Table 1 VMware releases

Product	Release
vSAN Advanced	6.7
Poweredge R740xd	vSAN Ready Node
ESXi	6.7
vCenter Standard	6.7
vRealize Suite Advanced	6.7
vRealize Orchestration Log Insight	7.5
vSphere Enterprise plus	6.7

Table 2 ECS releases

Product	Version
ECS	3.2
GeoDrive	1.2.2.1

Table 3 Genetec Security Center releases

Release	Subrelease
Genetec Security Center	5.7 SR2
	5.7 SR1

VMware vSphere

VMware vSphere is a virtualization platform that is used across thousands of IT environments around the world. VMware vSphere can transform or virtualize computer hardware resources, including CPU, RAM, hard disk, and network controller, to create a fully functional virtual machine (VM) that runs its own operating systems and applications like a physical computer.

The high-availability features of VMware vSphere coupled with VMware vSphere Distributed Resource Scheduler (DRS) and VMware vSphere Storage vMotion enable the seamless migration of virtual desktops from one ESXi server to another with minimal or no impact to the customer's usage.

VMware vCenter High Availability

VMware vCenter High Availability is feature of vSphere and uses a four-node cluster. The vCenter High Availability provides protection from downtime and uninterrupted failover and failback.

VMware vSAN

VMware vSAN aggregates local or direct-attached data storage devices to create a single storage pool shared across all hosts in the vSAN cluster. vSAN eliminates the need for external shared storage, and simplifies storage configuration and virtual machine provisioning.

vSAN is a distributed layer of software included in the VMware ESXi hypervisor, and it is fully integrated with VMware vSphere. vSAN supports vSphere features that require shared storage, such as High Availability (HA), vMotion, and Distributed Resource Scheduler (DRS). VM storage policies enable you to define VM storage requirements and capabilities.

Each host in a vSAN cluster contributes storage to the cluster. These storage devices combine to create a single vSAN datastore.

Dell EMC PowerEdge Ready Nodes

Dell EMC vSAN Ready Nodes are pre-configured and validated building blocks that can reduce deployment risks, improve storage efficiency, and let you quickly and easily scale storage as needed.

Dell EMC vSAN Ready Nodes are built on Dell EMC PowerEdge R740xd and R440 servers that have been pre-configured, tested, and certified to run VMware vSAN. Each Ready Node includes the right amount of CPU, memory, network I/O controllers, HDDs, and SSDs that are suited for VMware vSAN.

VMware Pulse IoT Center

VMware Pulse IoT Center is a secure, enterprise-grade IoT device management and monitoring solution. Integrate, manage, monitor and secure IoT use cases from the edge to the cloud, bridge the gap between Information Technology and Operational Technology organizations and simplify IoT device management with Pulse IoT Center.

VMware vRealize Operations Manager

VMware vRealize Operations Manager delivers intelligent operations management with application-to-storage visibility across physical, virtual, and cloud infrastructures. Using policy-based automation, operations teams automate key processes and improve IT efficiency.

Using data collected from system resources (objects), vRealize Operations Manager identifies issues in any monitored system component, often before the customer notices a problem. vRealize Operations Manager also frequently suggests corrective actions you can take to fix the problem right away. For more challenging problems, vRealize Operations Manager offers rich analytical tools that allow you to review and manipulate object data to reveal hidden issues, investigate complex technical problems, identify trends, or analyze to gauge the health of a single object.

VMware surveillance software editions

VMware vRealize Operations Manager delivers intelligent operations management with application-to-storage visibility across physical, virtual, and cloud infrastructures. Using policy-based automation, operations teams automate key processes and improve IT efficiency.

IoT Management and Monitoring

VMware Pulse IoT Center

- vSAN
- vSphere
- vCenter

vRealize Log Insight

Intelligent log management and analytics

For more information about configuring VMware vSAN, vSphere and vCenter solutions see:

- Administering VMware Virtual SAN
- VMware vSphere Update Manager Documentation
- About vCenter Server Appliance Configuration

For more information about Pulse IoT Center, see Pulse IoT Center Datasheet.

Dell EMC ECS

Dell EMC ECS is a complete software-defined cloud storage platform that supports the storage, manipulation, and analysis of video surveillance and unstructured data on a massive scale on commodity hardware. ECS is specifically designed to support the mobile, cloud, and Big Data workloads that are similar to large-scale surveillance workloads.

Retention periods and policies

ECS provides the ability to prevent data from being modified or deleted within a specified retention period. Bucket based retention is not supported and should not be used with any VMS when using the CIFS-ECS service. VMS time based retention is the only supported retention policy when using CIFS-ECS.

Cluster Capacity

Dell EMC only supports the use of time based retention settings with the VMS. To determine the capacity requirement for each recorder, calculate the number of cameras per recorder, the target bit rate per camera, and the retention time in days. Always consult with the VMS ISV to determine an accurate capacity estimate.

All writes to the ECS cluster stop when the cluster capacity reaches 90% full. It is always recommended to plan for additional capacity as soon as you reach 75% of the cluster capacity.

Quotas

When using GeoDrive, Dell EMC requires the use of ECS soft quotas. Quotas are the storage space limit that is specified for the ECS buckets. You can specify a storage limit for the bucket and define notification and access behavior when the quota is reached. The quota setting for a bucket cannot be less than 1 GB and can be specified in increments of 1 GB.

The Dell EMC Surveillance Lab recommends only using soft quotas for surveillance. Dell EMC recommends maintaining 15% overhead beyond the capacity requirement.

The quota behavior options are as follows:

Notification Only at *<quota_limit_in_GB>*

Soft quota setting at which you are notified.

Block Access Only at *<quota_limit_in_GB>*

Hard quota setting which, when reached, prevents write/update access to the bucket.

Block Access at *<quota_limit_in_GB>* and Send Notification at *<quota_limit_in_GB>*

Hard quota setting which, when reached, prevents write/update access to the bucket and the percentage of the quota setting at which you are notified.

Garbage collection

Garbage collection in ECS is designed such that it runs with lower priority than input/ output activity. When an object is deleted, ECS waits for garbage collection to reclaim the space allocated to that object. However, the object is marked as deleted and the deletion is reflected in the user's view of system utilization through metering and chargeback reports.

An object maps to a set of chunks as all data is stripped and spread across the chunks during data ingest. Therefore, a single object and its metadata could span multiple data chunks and metadata chunks. Each chunk has a logical volume of 128 MB. Processing a delete requires updates to the object index as well as the chunk index. Garbage collection verification is performed to ensure that all object references to a chunk have been removed before it is marked for reclamation. Chunks that pass the verification are then reclaimed through the garbage collection process.

There two types of garbage collection, Repo GC and Btree GC. Each has two types of GC Full GC and partial GC. Full GC is when chunk has no references of objects - it is eligible for full GC. When more than 2/3 of the chunk is garbage, garbage collection does not wait until the remaining 1/3 becomes garbage before processing. Partial GC frees up the chunk by merging valid data of such chunks.

To protect users from data loss in the event of accidental deletion, the steps in the deletion and space reclamation process are not performed in quick succession.

Dell EMC recommends tuning the garbage collection process for video surveillance workloads to achieve faster space reclamation. The parameters to tune are:

- Decrease the time interval for the frequency of verification scanner
- Increase the scanner throttle for number of objects
- Increase the scan tasks expiration times
- Increase the maximum number of pending partial GC tasks

Please contact Dell EMC ECS technical support for more information about tuning these parameters.

Dell EMC GeoDrive

The Dell EMC GeoDrive tool provides a local file system interface through which you can store and retrieve files on Dell EMC ECS Object Storage. Use GeoDrive to store and retrieve files, such as pictures, movies and documents, in the cloud using the same applications and tools that you use today.

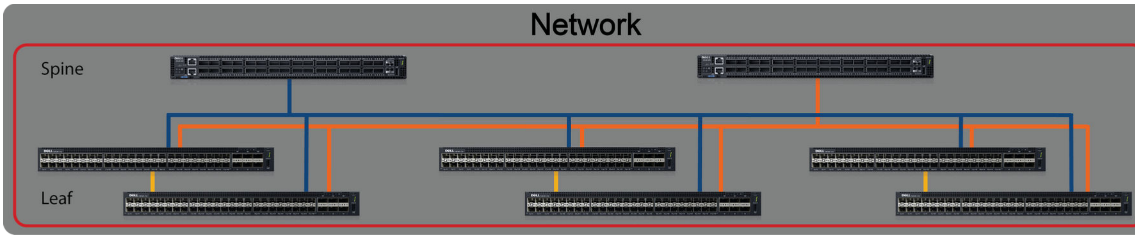
Refer to the Dell EMC CIFS-ECS Tool User Guide for information about installation and configuration of GeoDrive on the recorder.

Network

Surveillance is an end-to-end solution that is connected using a simplistic to complex network infrastructure. A typical solution spans multiple network layers, ranging from the access layer providing power over Ethernet (PoE) for video cameras, to the data center that provides the centralized network that is used to interconnect all of the surveillance components.

With cameras on the edge, the data center infrastructure is made of aggregation switches that are known as leaf switches, and a core switch, which is known as the spine. A small campus network has an aggregation layer, but not a data center or core. The network must be correctly sized in terms of capacity, efficiency, and resilience to effectively resolve the user's business challenges.

Figure 3 Network spine and leaf configuration

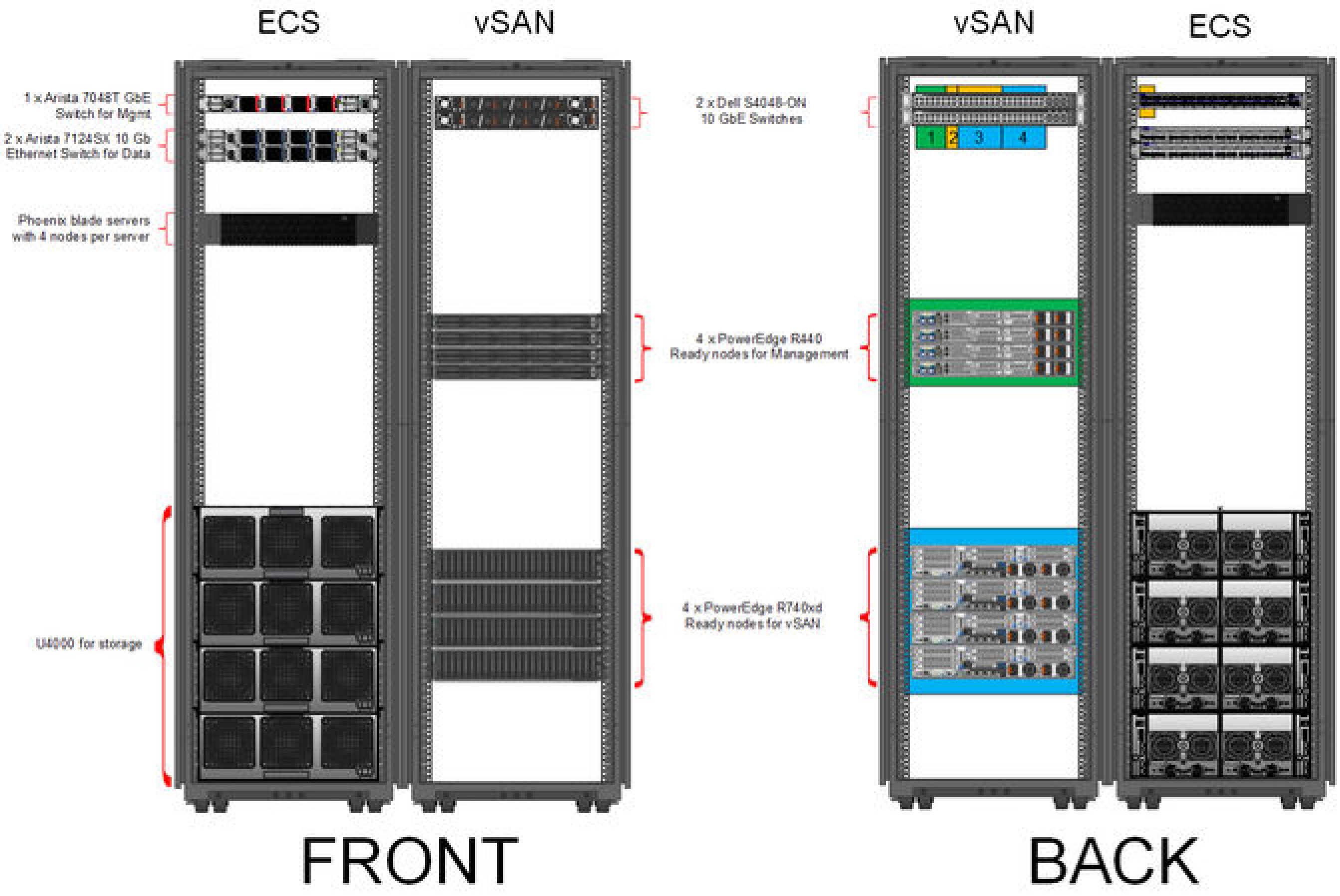


Connecting the vSAN and ECS nodes

The vSAN management nodes, vSAN surveillance nodes and ECS nodes are not connected internally and must be integrated through external switches. Each node should be connected to 2 physical switches to ensure redundancy and avoid a single point of failure.

The following figure shows the standard configuration for the ECS and vSAN racks and a basic connection overview for the switches.

Figure 4 Dell EMC ECS and VMware vSAN rack configuration

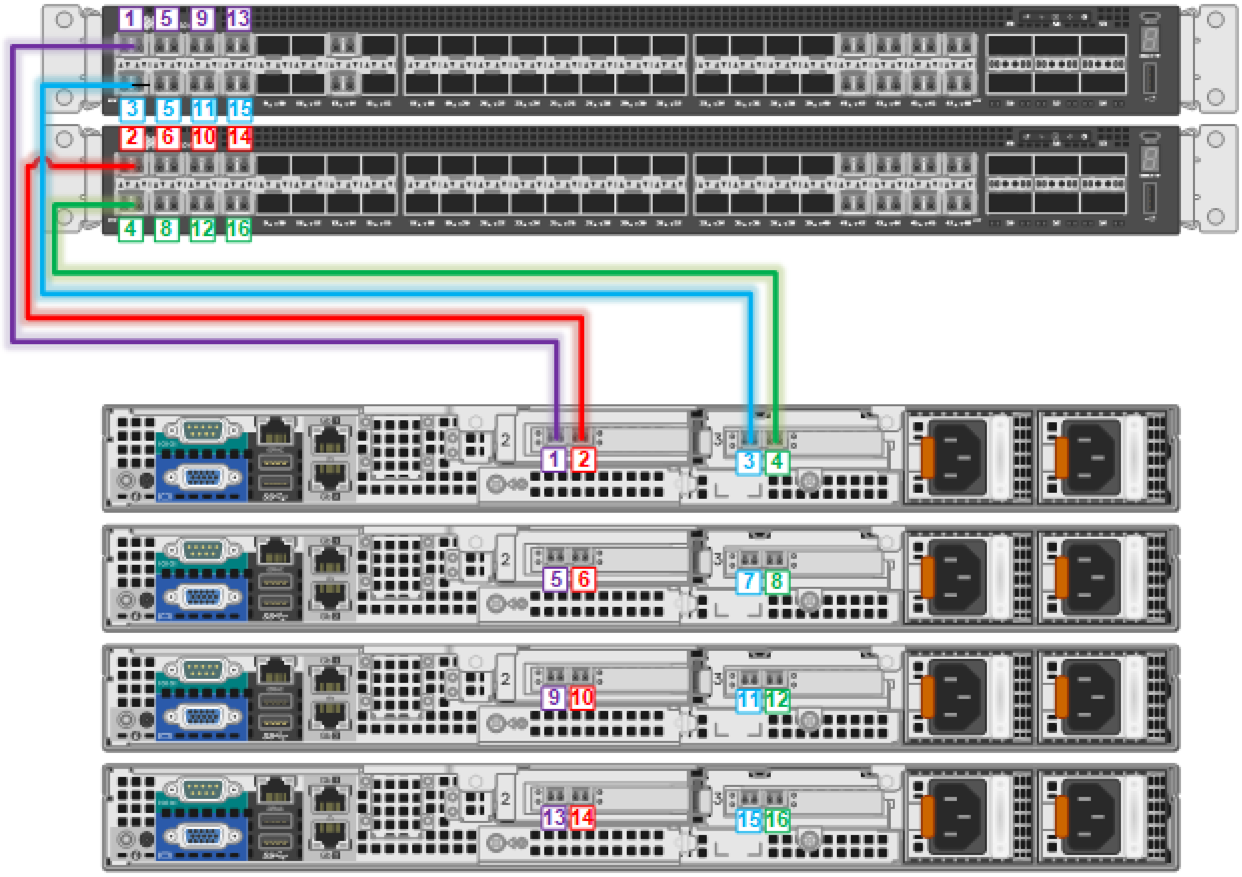

ECS
vSAN
vSAN
ECS
1 x Arista 7048T GbE Switch for Mgmt
2 x Arista 7124SX 10 Gb Ethernet Switch for Data
Phoenix blade servers with 4 nodes per server
U4000 for storage
2 x Dell S4048-ON 10 GbE Switches
1
2
3
4
4 x PowerEdge R440 Ready nodes for Management
4 x PowerEdge R740xd Ready nodes for vSAN
FRONT
BACK

1. Ports 01-12 = Management: Populate ports left to right
2. Ports 13-16 = ECS: Populate ports left to right.
3. Ports 17-32 = Additional ECS or vSAN Nodes: Populate ports left to right
4. Ports 33-48 = vSAN nodes: Populate ports right to left

Connecting the vSAN management cluster

Connect the vSAN management nodes to the network starting with ports 1 and 2 on the switch. Add additional management nodes using open ports in ascending order (left to right) on the switch, as shown in the following figure.

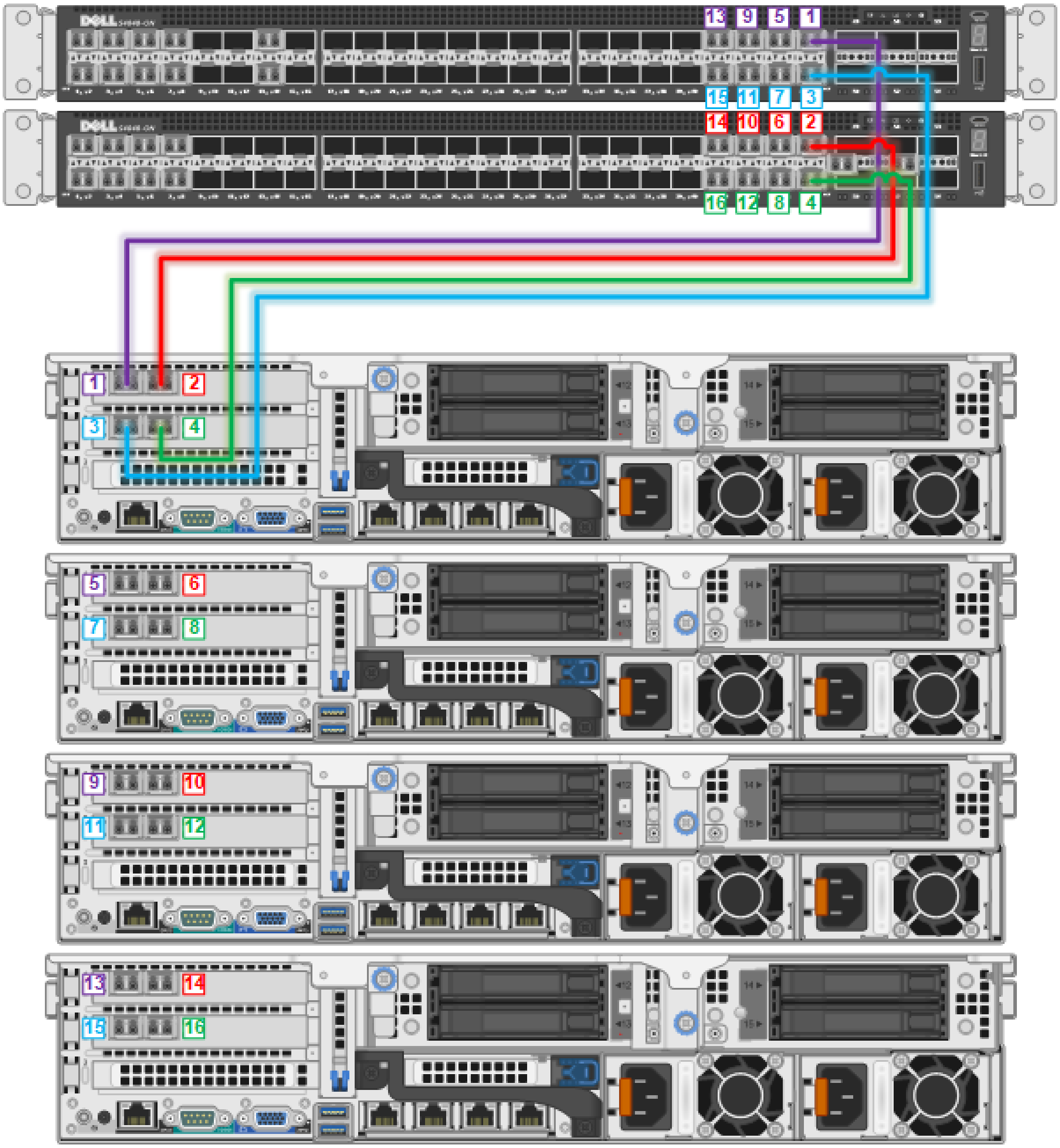
Figure 5 vSAN management node cabling diagram



Connecting the vSAN surveillance nodes

Connect the vSAN surveillance nodes to the network starting with ports 47 and 48 on the switch. Add additional surveillance nodes using open ports in descending order (right to left) on the switch, as illustrated in the following figure.

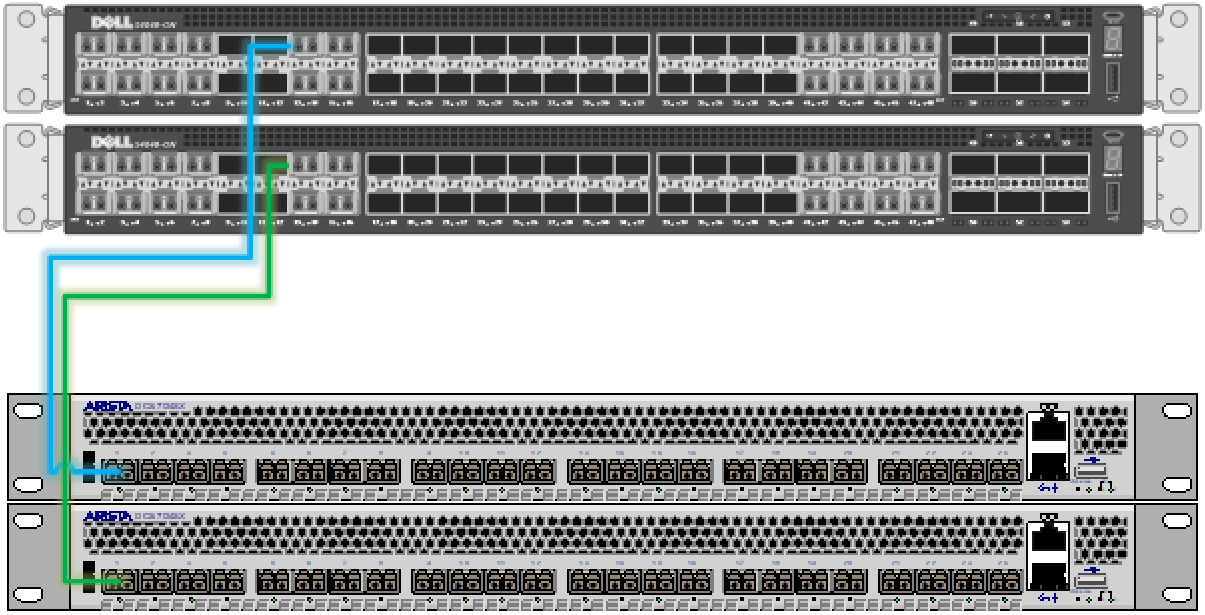
Figure 6 vSAN surveillance node cabling diagram



Connecting the ECS

Connect the ECS cabinet to the vSAN through the network switch starting with port 13 on both switches, as illustrated in the following figure. Add additional ECS cabinets using open ports in ascending order (left to right) on the switch starting with port 14.

Figure 7 ECS to vSAN cabling diagram



CHAPTER 3

Conclusion

This chapter presents the following topics:

Summary

The Dell EMC Surveillance Lab performed comprehensive testing with Genetec Security Center against VMware vSAN and Dell EMC ECS Object Storage.

Depending on the implementation needs, you can use Dell EMC storage for Genetec Security Center.

The Genetec architecture and product suite allows extreme scaling, from a few cameras to up to tens of thousands of cameras, by using Dell EMC storage.

ECS storage

Dell EMC ECS is a software-defined, cloud-scale, object storage platform that combines the cost advantages of commodity infrastructure with the reliability, availability and serviceability of traditional arrays. With ECS, any organization can deliver scalable and simple public cloud services with the reliability and control of a private-cloud infrastructure.