Infraestructura hiperconvergent en la industria farmacèutica

Àrea: Administració de xarxes i sistemes operatius

Alumne: **Adrian José Antón Gonzalvez**

Versió: **1.0**

Índex

1 INTRODUCCIÓ 6
1.1 DESCRIPCIÓ DEL PROJECTE 6
1.2 MOTIVACIÓ PER REALITZAR EL PROJECTE 6
1.3 ÀMBIT D´APLICACIÓ DEL PROJECTE 6
1.4 OBJECTIUS DEL PROJECTE 6
1.5 CRONOGRAMA DEL TFG 7
1.6 DIAGRAMA DE GANTT 8
2 ANÀLISIS I ESTUDI TECNOLÒGIC 9
2.1 INTRODUCCIÓ 9
2.2 SOLUCIÓ HIPERCONVERGENT VS CONVERGENT 9
2.3 ELECCIÓ DEL PROVEÏDOR I ANÀLISIS DE MERCAT 10
2.3.1 Lideratge al mercat 10
2.3.2 Solidesa i idoneïtat del portafolis de productes 10
2.3.3 Abast, flexibilitat i accessibilitat de suport 12
2.3.4 Facilitat de compra 13
2.3.5 Resum i elecció final 13
3 ESTÀNDARD DE CONNECTIVITAT DE XARXA 15
3.1 INTRODUCCIÓ 15
3.1.1 Objectiu 15
3.1.2 Abast 15
3.2 DISSENY FÍSIC DE XARXA 15
3.2.1 Nomenclatura dispositius de xarxa 15
3.2.2 Adreçament de xarxa 16
3.2.3 Inventari d'equips de xarxa 17
3.2.4 Diagrama físic de xarxa 18
3.3 DISSENY LÒGIC DE LA XARXA 18
3.3.1 Topologia 18
3.3.2 Tipus de xarxes 19
3.3.3 Definició de les VLAN's 19

3.3.4 Tipus de firewalls ... 20
3.3.5 Segmentació de xarxa ... 20
3.3.6 Diagrama lògic de xarxa ... 21
4 INFRAESTRUCTURA VIRTUAL HIPERCONVERGENT ... 22
4.1 INTRODUCCIÓ ... 22
4.1.1 Visio general ... 22
4.2 GENERALITATS DE L'ENTORN ... 23
4.2.1 Solució hiperconvergent VxRail Dell ... 23
4.2.2 Infraestructura instal·lada ... 24
4.3 CONFIGURACIÓ DE XARXA ... 25
4.3.1 Configuració switchos TOR ... 26
4.4 CONFIGURACIÓ DEL CLUSTES VXRAIL ... 29
4.4.1 Components del clúster ... 31
4.4.2 Configuració DNS ... 31
4.4.3 Configuració NTP ... 31
4.5 CONFIGURACIÓ DE LES INTERFÍCIES ... 31
4.5.1 Configuració interfícies físiques iDRAC ... 31
4.5.2 Configuració interfícies ESXi per a la gestió ... 32
4.5.3 Configuració interfícies vSAN ... 33
4.5.4 Configuració interfícies VMotion ... 36
4.5.5 Internal Managment ... 37
4.5.6 Configuració VDS Network Portgroups ... 37
4.6 COMPONENTS DE VXRAIL ... 39
4.6.1 VxRail Manager ... 39
4.6.2 vCenter ... 40
4.6.3 vSphere Cluster Services (vCLS) ... 44
4.6.4 vRealize LogInsight ... 45
5 SISTEMA DE BACKUPS OT ARCSERVE ... 48
5.1 INTRODUCCIÓ ... 48
5.2 SOLUCIÓ PROPOSADA ... 48
5.3 GENERALITATS DEL ENTORN ... 49
5.3.1 Appliance Arcserve ... 49
5.3.2 Cabina Immutable OneXafe ... 50

5.3.3 Arcserve UDP 52
5.3.4 Deduplicació Arcserve 53
5.3.5 Funcionament dels plans a Arcserve 56
5.3.6 Mètodes de backup 57
5.4 PLANS COPIES DE SEGURETAT 58
5.4.1 Replicació backups Arcserve 58
5.4.2 Configuració plans 58
6 GLOSSARI 62

1 INTRODUCCIÓ

1.1 DESCRIPCIÓ DEL PROJECTE

Actualment la digitalització és cada vegada més important en la indústria farmacèutica perquè permet a les empreses millorar l'eficiència i la qualitat en tots els aspectes de la seva operació, des de la recerca i el desenvolupament de nous medicaments fins a la producció i la distribució.

Per tant des de el departament d'Automatització, es vol impulsar un programa de treball i transformació cap a una infraestructura hiperconvergent (HCI) per alinear la tecnologia amb els pilars estratègics.

Una infraestructura HCI és un sistema unificat i definit per programari que aplega tots els elements d'un centre de dades tradicional: emmagatzematge, recursos de còmput, xarxa i gestió. Aquesta solució integrada utilitza programari i servidors per substituir les solucions convencionals amb cabines de discos, reduint la complexitat del centre de dades i incrementant-ne l'escalabilitat.

1.2 MOTIVACIÓ PER REALITZAR EL PROJECTE

El motiu principal de la realització d'aquest TFG, es la necessitat de alinear el sistemes informàtics del entorn industrial, específicament en el sector farmacèutic, amb les ultimes tecnologies, en entorns farmacèutics pel fet que les dades que es manegen en aquest sector són crítics i sensibles, com la informació sobre la investigació, desenvolupament i producció de medicaments, dades de pacients, informació financera i propietat intel·lectual.

A mes a mes, com que estem parlant del entorn de fabricació GMP (Good Manufacturing Practice), hem de garantir la qualitat, seguretat i eficàcia dels productes farmacèutics, i ha d'incloure aspectes com el disseny i control del procés, la qualificació i el manteniment de l'equip, el control de la qualitat, la capacitació del personal, la documentació i registre, i el compliment normatiu.

1.3 ÀMBIT D´APLICACIÓ DEL PROJECTE

La infraestructura proposada en aquest projecte es pot aplicar a qualsevol àmbit de fabricació industrial, ja que implementem la virtualització d'entorns d'automatització i control de processos en entorns hiperconvergents per oferir el rendiment adequat, garantir la disponibilitat del procés i la flexibilitat per adaptar-se a requeriments nous de forma transparent.

1.4 OBJECTIUS DEL PROJECTE

L'objectiu principal d'aquest projecte es construir la base que permeti que les operacions de la planta industrial siguin segures, definint tant l'arquitectura de xarxa, com la virtualització i els sistemes de copies de seguretat, adaptades a les exigències dels entorns de control de processos, reduint els temps de latència i la probabilitat d'una para de planta no controlada.

1.5 CRONOGRAMA DEL TFG

En el següent cronograma indiquem les setmanes durant les quals es realitzarà el TFG, també les activitats que farem durant aquestes setmanes, que finalitzarem amb l'entrega final del TFG, que esta planificada per la setmana del 29 de Maig al 4 de Juny de 2023:

TFG			
	Setmana	**Activitat**	**Comentaris**
1	1-mar 05-mar	Inici proposta del pla de treball del TFG	
2	06-mar 12-mar		
3	13-mar 19-mar	Proposta TFG	Lliurament PAC1
4	20-mar 26-mar	Estudi arquitectura de xarxa a implementar	
5	27-mar 02-abr	Definició dels estàndards de connectivitat	
6	3-abr 09-abr	Revisió i correccions	
7	10-abr 16-abr	Estudi de la solució hiperconvergent	
8	17-abr 23-abr	Estàndard de connectivitat de xarxa + Inici solució hiperconvergent	Lliurament PAC2
9	24-abr 30-abr	Definició del entorn virtual hiperconvergent	
10	01-may 07-may	Revisió i correccions	
11	15-may 21-may	Definició de la solució de copies de seguretat + Revisió i correccions	
12	22-may 28-may	-	Preparatius y documentació de annexos i bibliografia
-	Entrega documentació 80-90% TFG	Lliurament PAC3	
13	29-may 4-jun (*)	-	Revisió i correccions
-	Conclusió final		
-	Entrega final Memòria i Presentació	Entrega final	
14	05-jun 11-jun		
15	12-jun 18-jun	Període de consulta del Tribunal (dates a	

1.6 DIAGRAMA DE GANTT

2 ANÀLISIS I ESTUDI TECNOLÒGIC

2.1 INTRODUCCIÓ

La transformació digital ha esdevingut una imperativa comercial, ja que la majoria dels aspectes de la participació econòmica s'han tornat digitals. Arreu del món, les empreses i els organismes governamentals estan redissenyant les seves infraestructures de tecnologia per mantenir-se al mateix temps de les exigències dels clients, impulsar la innovació i continuar sent competitius en una economia digital en constant evolució.

Una enquesta recent de PwC va destacar que el 45% dels executius del negoci i de TI de 51 països identifica com una prioritat màxima l'augment dels ingressos per mitjà de la transformació digital. L'èxit en aquest panorama digital accelerat requereix que les empreses transformin les infraestructures de TI per assolir nous nivells de flexibilitat i de capacitat de resposta. Alhora, els equips de TI han d'aconseguir un equilibri entre mantenir els aspectes principals del negoci mentre inverteixen en noves innovacions de negocis i de tecnologia necessàries per competir en l'ambient dinàmic d'avui.

Els sistemes d'infraestructura hiperconvergent (HCI) agrupen diversos components de la tecnologia en sistemes en sistemes individuals, cosa que permet als departaments de TI dedicar menys temps a administrar els components de centres de dades separats i més temps a oferir valor al negoci proactivament. En aquest informe tècnic, comparem les ofertes del dossier de Dell EMC i HPE, i destaquem beneficis significatius que es poden aconseguir mitjançant l'associació amb el líder del mercat HCI: Dell EMC.

Dell EMC proporciona un ecosistema de programari estretament integrat i la flexibilitat d'executar diversos tipus de càrrega de treball, el que proporciona solucions per a una base de clients més àmplia de HPE.

2.2 SOLUCIÓ HIPERCONVERGENT VS CONVERGENT

Una de les maneres més lògiques i eficients per modernitzar la TI i impulsar el valor comercial incremental és aprofitar la infraestructura hiperconvergent. A continuació trobareu resums de la infraestructura convergent i la infraestructura hiperconvergent:

- **La infraestructura convergent (CI)** combina múltiples components de maquinari (servidor, emmagatzematge i xarxes) amb programari d'administració que ofereix organització, que en general es lliura com un sol rack i es ven com un sol producte. Està preconfigurat segons les càrregues de treball que admet, per la qual cosa no es pot alterar significativament la configuració després de la instal·lació.
- **L'arquitectura hiperconvergent (HCI)** és una arquitectura definida per programari amb processament, emmagatzematge definit per programari, virtualització i (sovint) xarxes integrades. Per tant, la configuració és més flexible, ja que no depèn del maquinari tant com amb la infraestructura convergent (CI).

Tot i que tots dos tenen els seus mèrits, ens centrarem en HCI, ja que representa un dels segments de creixement més ràpid en TI en l'actualitat. El motiu pel qual més organitzacions estan incorporant HCI al centre de dades és que una quantitat cada vegada

més gran de càrregues de treball es beneficien de l'escalament horitzontal de l'emmagatzematge i el processament mitjançant una tecnologia d'emmagatzematge definit per programari de base en una arquitectura hiperconvergent. HCI redueix els costos operacionals mitjançant la unificació de l'administració de l'emmagatzematge i el processament, cosa que redueix el cost total d'adquisició, cosa que millora l'accessibilitat d'HCI per a les organitzacions.

2.3 ELECCIÓ DEL PROVEÏDOR I ANÀLISIS DE MERCAT

Consideracions importants sobre la selecció d'un proveïdor d'HCI:

- **Lideratge al mercat:** fortaleses a llarg termini del proveïdor per suportar el cicle de vida del producte i brindar excel·lència en la solució.
- **Solidesa i idoneïtat del portafoli de productes**: apropiat per a la solució requisits del negoci i de càrrega de treball múltiples o variats.
- **Abast, flexibilitat i accessibilitat de suport:** la capacitat de recolzar i sustentar l'eficàcia de les solucions en un clima de negoci en canvi constant.
- **Facilitat de compra**: disponibilitat dels termes financers i models de consum més estratègics per al negoci del client.

2.3.1 Lideratge al mercat

IDC (International Data Corporation) identifica Dell EMC com el proveïdor número 1 a l'espai hiperconvergent amb el 30.6 % de la quota de mercat, mentre que HPE queda enrere al número 4 amb només el 3.6 % de quota de mercat. A més, les trajectòries dels dos proveïdors semblen dirigir-se en adreces oposades; mentre que Dell EMC ha augmentat la seva quota en els darrers sis trimestres, HPE ha perdut la seva quota de mercat cada trimestre dur davant del darrer any 2022. És important destacar que a l'espai d'HCI, on el mercat general va créixer un 68% any rere any, els ingressos de Dell EMC van créixer més ràpid que el mercat a un 158% interanual, mentre que HPE va tenir el creixement més lent dels cinc proveïdors principals, amb només un 8,8% interanual.

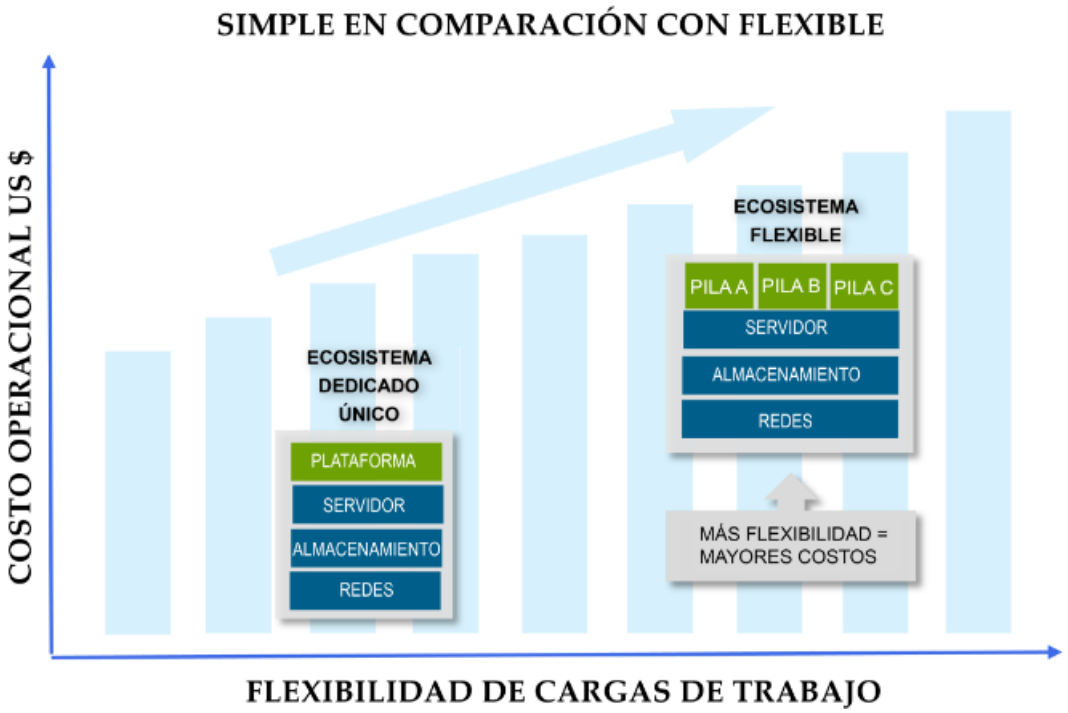
Aquests resultats de mercat indiquen clarament les preferències dels clients i la capacitat del proveïdor per oferir els resultats necessaris en comprar una solució HCI i destaquen factors importants que han de considerar les organitzacions de TI: Tecnologia, serveis, suport i finançament.

2.3.2 Solidesa i idoneïtat del portafolis de productes

Els centres de dades definits per programari (SDDC) poden oferir estalvis de costos, guanys en eficiència, consolidació, millores a l'administració i automatització. Perquè una organització arribi al punt en què puguin collir completament aquests beneficis, han de prendre decisions que, en la majoria dels casos, inclouen desavantatges. Una de les

decisions més importants en triar un enfocament de centre de dades definit per programari és equilibrar la flexibilitat amb la simplicitat.

En un SDDC, un ecosistema dedicat únic (p. ex., VMware) simplifica l'administració, integració i organització a tota la pila de programari, cosa que resulta en reduir els costos operacionals. Aquest enfocament, però, requereix que les càrregues de treball es regeixin per les regles d'un ecosistema particular. D'altra banda, un ecosistema flexible compatible amb múltiples hipervisors, o fins i tot càrregues de treball de baix nivell, permet a TI admetre més tipus de càrregues de treball i aplicacions sense afegir més complexitat a l'ambient. Això redueix els costos de configuració, integració i suport. No hi ha un enfocament "correcte" per a aquesta pregunta de flexibilitat o simplicitat; tot depèn de les necessitats del client i el tipus de càrrec de treball que desitgen a dimitir.

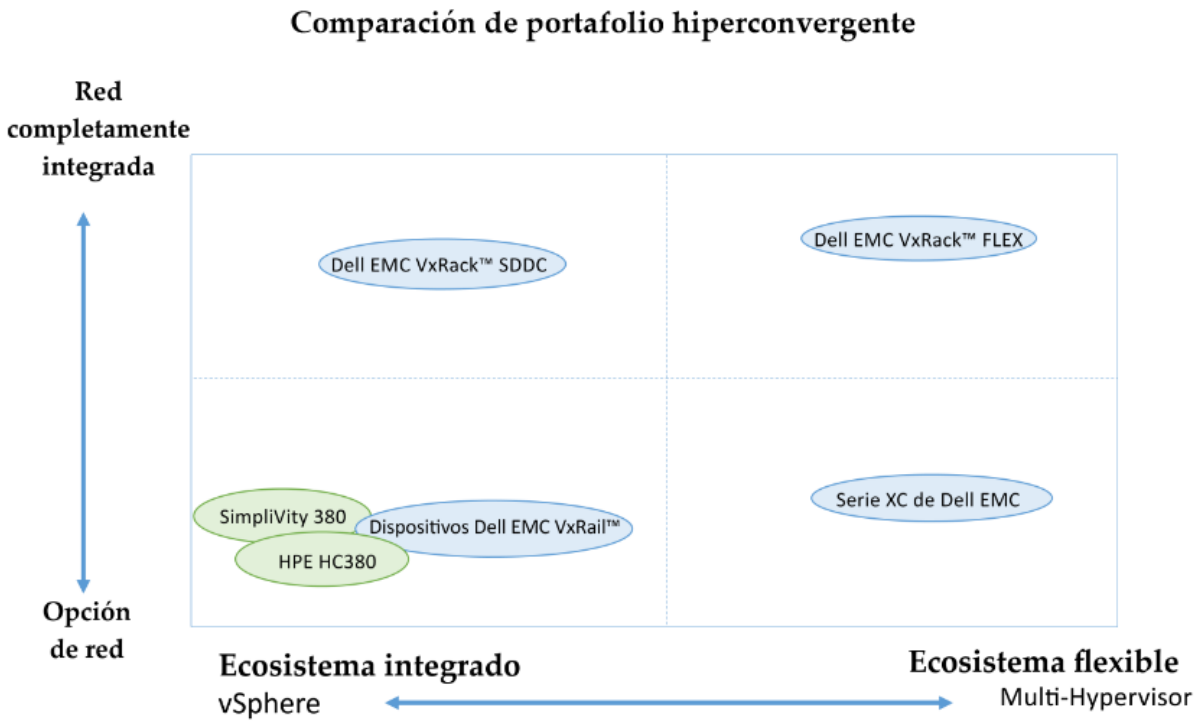


En comparar els dossier d'HCI de Dell EMC i HPE (el seu competidor principal), podem identificar dos enfocaments HCI diferents:

- **Dell EMC** ofereix l'elecció d'un ecosistema d'únic o un ecosistema flexible. Això permet que els clients triïn una solució que s'ajusti més estretament als requisits de càrrega de treball.

- **HPE** només ofereix un enfocament d'ecosistema integrat. Això limita les opcions dels clients.

El portafoli HCI de Dell EMC proporciona als clients l'elecció d'integrar-se completament a la pila de virtualització de VMware o la flexibilitat d'escollir diferents ambients de virtualització i integració de xarxa. HPE ofereix un sol enfocament amb dos tipus diferents de dispositius que es basen en vSphere, però no integrats tan estretament a tota la plataforma VMware com Dell EMC.



L'enfocament de HPE als dispositius de HCI és limitat en termes de compatibilitat d'hipervisor, configuracions de maquinari i escalabilitat si es comparen amb les configuracions de maquinari, la tecnologia de SDS, la densitat i l'escalabilitat disponibles al dossier de dispositius de HCI de Dell EMC, hi ha una quantitat significativament més gran d'opcions en comparació amb HPE.

Per exemple:

- Els dispositius VxRail de Dell EMC poden escalar a 64 nodes, mentre que HPE només pot escalar a 32.
- La combinació de VxRail de Dell EMC i la sèrie XC ofereix dotze diferents models, mentre que HPE n'ofereix només tres.
- La sèrie XC de Dell EMC ofereix funcionalitats de múltiples hipervisors, mentre que HPE no compta amb un model que ofereixi funcionalitats de múltiples hipervisors.

2.3.3 Abast, flexibilitat i accessibilitat de suport

Amb la convergència de maquinari i programari en les solucions de HCI, és extremadament important comptar amb una cobertura de suport adequada per evitar sorpreses. Els proveïdors d'infraestructura tradicional poden oferir suport de programari i maquinari per separat, per la qual cosa recomanem treballar amb un proveïdor que pugui brindar suport a tot la solució i que tingui associacions d'ecosistema sòlides que admetin i optimitzin la solució per tot el seu cicle de vida.

Els serveis de suport per a clients de Dell EMC van ser avalats per Technology Services Industry Association (TSIA) per centrar-se a assegurar-se que els clients rebin els millors resultats amb la tecnologia. El dossier integral de ProSupport Enterprise Suite i de ProDeploy Enterprise Suite simplifica el procés de selecció del nivell adequat de servei i

suport per a solucions de TI, inclosos maquinari, programari, amb objectius de resposta de destinació de missió crítica.

Si bé HPE ofereix una cobertura de suport similar, els clients han de navegar diverses opcions de suport de maquinari i programari per crear el paquet d'implementació i suport adequat per a les vostres necessitats. L'enfocament de Dell EMC de " empaquetar " les funcions d'implementació i suport més comunament necessàries elimina gran part de la incertesa en seleccionar el nivell adequat de servei de suport i redueix els costos de manteniment.

2.3.4 Facilitat de compra

Com a part dels seus dossier de finançament, Dell EMC i HPE tenen programes de pagament flexibles que permeten a les empreses pagar a mesura que consumeixen emmagatzematge, per la qual cosa paguen només el que usen, el que redueix les despeses de capital inicials. D'altra banda, dins l'espai del dispositiu de HCI, Dell EMC i HPE ofereixen programes específics de pagament flexibles pensats per facilitar la transició a HCI mentre que limiten el risc financer associat amb grans inversions de TI.

2.3.5 Resum i elecció final

La Infraestructura Hiperconvergent ofereix una ruta convincent per als departaments de TI que busquen transformar les seves infraestructures per a més agilitat, simplicitat, rendiment i escalabilitat, a més d'una rendibilitat significativa. Principalment:

- HCI permet a departaments que siguin flexibles i àgils en bregar amb els requisits de càrregues de treball combinades i les aplicacions natives del núvol.
- HCI permet als clients començar amb poc i escalar segons les seves necessitats, cosa que redueix els riscos financers i permet la capacitat d'augmentar segons els requisits del negoci.

Dell EMC i HPE ofereixen alternatives de HCI. Tot i això, Dell EMC ofereix un portafoli més ampli d'opcions d'ecosistemes únics o flexibles, serveis de suport reconeguts i plans de pagament més flexibles.

El portafoli de Dell EMC inclou els dispositius d'HCI amb opcions d'integració d'hipervisor i de xarxa, mentre que HPE només ofereix dispositius que funcionen amb un sol hipervisor i no una xarxa integrada, cosa que limita considerablement les opcions perquè els clients puguin adaptar-se a les seves necessitats de càrregues de treball i fer un escalament vertical o horitzontal.

Els dispositius VxRail de Dell EMC, amb tecnologia de processadors escalables Intel® Xeon® i desenvolupats en conjunt amb VMware, i la relació d'OEM de la sèrie XC amb Nutanix (els dos proveïdors principals d'emmagatzematge definit per programari) diferencien Dell EMC de la resta, ja que els dispositius de HPE es basen en la tecnologia de propietat de SimpliVity. A més, en proves de rendiment que van comparar els dispositius VxRail amb HC380 i SimpliVity, VxRail va superar en rendiment ambdós sistemes de HPE.

Per tant, després d'aquest anàlisis de mercat hem decidit implementar una solució hiperconvergent amb el producte VxRail de Dell EMC.

3 ESTÀNDARD DE CONNECTIVITAT DE XARXA

3.1 INTRODUCCIÓ

3.1.1 Objectiu

L'objectiu del present apartat, és definir l'arquitectura de xarxa del entorn industrial, dissenyat per protegir l'entorn contra accessos i comportaments indeguts, adaptant l'arquitectura de control al paradigma de seguretat actual, seguint els estàndards i les bones pràctiques definides per la norma IEC/ISA62443 i el NIST 800-82.

Les bones pràctiques en segmentació s'han desenvolupat segons el marc per a la segmentació de xarxa definida per l'estàndard ISA99/IEC62443, desenvolupat pel Comitè de la Societat Internacional d'Automatització (ISA) i adoptat per la Comissió Electrotècnica Internacional (IEC), el qual constitueix el principal marc de referència internacional de ciberseguretat industrial per abordar i mitigar les vulnerabilitats de seguretat actuals i futures als sistemes d'automatització i control industrial (IACS).

3.1.2 Abast

L'abast del present capítol és definir el disseny físic i lògic de la xarxa OT industrial, tenint en compte els següents axiomes:

- Adaptació de l'arquitectura de control al paradigma de seguretat actual.
- Adaptació dels estàndards i bones pràctiques definides a l'IEC62443 i al NIST 800-82.
- Protegir l'entorn industrial contra accessos i comportaments indeguts.
- Millora en la resposta a incidents de seguretat.
- Reducció del soroll de xarxa i trànsit broadcast.
- Restricció del trànsit entre cel·les/processos. Bloqueig de moviments laterals.
- Estandardització de l'encaminament. Creixement il·limitat.
- Definició de les polítiques d'encaminament i control d'accés a les diferents capes de comunicació (DMZ, xarxes IT, DMZ Industrial i zones de control de processos).

3.2 DISSENY FÍSIC DE XARXA

3.2.1 Nomenclatura dispositius de xarxa

A continuació, s'inclou una proposta de sintaxi de nomenclatura atenent les necessitats observades a l'entorn industrial:

AABBBCDDEEFFFF

- AA País on s'ubica el dispositiu d'acord amb l'estàndard UN/LOCODE (la part del país coincideix amb la norma ISO 3166-1 alpha-2)
    - En cas que els servidors estiguin allotjats en un servei Cloud, s'utilitzaran les inicials següents: ME (Middle East), EU (Europe), US (EUA), AP (Àsia Pacific), segons ubicació.
- BBB Ciutat on s'ubica el dispositiu d'acord estàndard UN/LOCODE.
    - En cas que els servidors estiguin allotjats en un servei Cloud i donin servei a més d'una seu, es faran servir les inicials dels Headquarters
- C Identificador numèric de la seu dins la ciutat on hi ha l'equip. Aquest identificador s'inclou per si hi ha diverses ubicacions a la mateixa localitat, cosa que actualment no passa.
- DD Xarxa a què pertany el dispositiu. Al principi, ens podríem trobar amb les opcions IT, OT o IO (IT/OT).
- EE Tipus d'element davant del qual ens trobem. Exemples: SW (switch), FW (Firewall), SV (server), PP (patch panell), RK (rack), PL (PLC), HM (HMI), PF (Perifèria), AP (Punt d'accés), ST (Storage), VL (VLAN), etc
- FFFF Identificador alfanumèric del dispositiu dins de la seu. Aquest ha de ser utilitzat per poder ubicar unívocament l'equip, per exemple, numerant consecutivament aquells que estan en una mateixa ubicació.

3.2.2 Adreçament de xarxa

Adreçament reservat: 10.14.128.0/17

- Xarxa sumaritzada DMZ: 10.14.128.0/19
- Xarxa sumaritzada Servicios: 10.14.160.0/19
- Xarxa sumaritzada Acces: 10.14.192.0/18

  o Xarxa sumaritzada monitoring: 10.14.192.0/20

  o Xarxa sumaritzada líneas: 10.14.208.0/20

  o Xarxa sumaritzada control: 10.14.224.0/19

    - DMZ

Subxarxa	Màscara	Descripció	Tipus
10.14.128.0	255.255.255.0	Xarxes de tránsit	Serveis
10.14.129.0	255.255.255.0	Jump Stations	Serveis
10.14.130.0	255.255.255.0	Serialització	Serveis

10.14.[131-140].0	255.255.255.0	Serveis infraestructura (Serveis DMZ, serveis de directori, Backups, FTP, intercambi de fitxers,…)	Serveis
10.14.142.0	255.255.255.0	MES	Serveis
10.14.143.0	255.255.255.0	Captor	Serveis
10.14.[144-159].0	255.255.255.0	Lliures	Serveis

- Serveis

Subxarxa	Màscara	Descripció	Tipus
10.14.[160-165].0	255.255.255.0	Gestió infraestructura	Serveis
10.14.[166-168].0	255.255.255.0	SCADA	Serveis
10.14.[169-191].0	255.255.255.0	Lliures	Serveis

- Accés

Subxarxa	Màscara	Descripció	Tipus
10.14.[192-255].0	255.255.255.0	Monitoring, Líneas y Control	Serveis

3.2.3 Inventari d’equips de xarxa

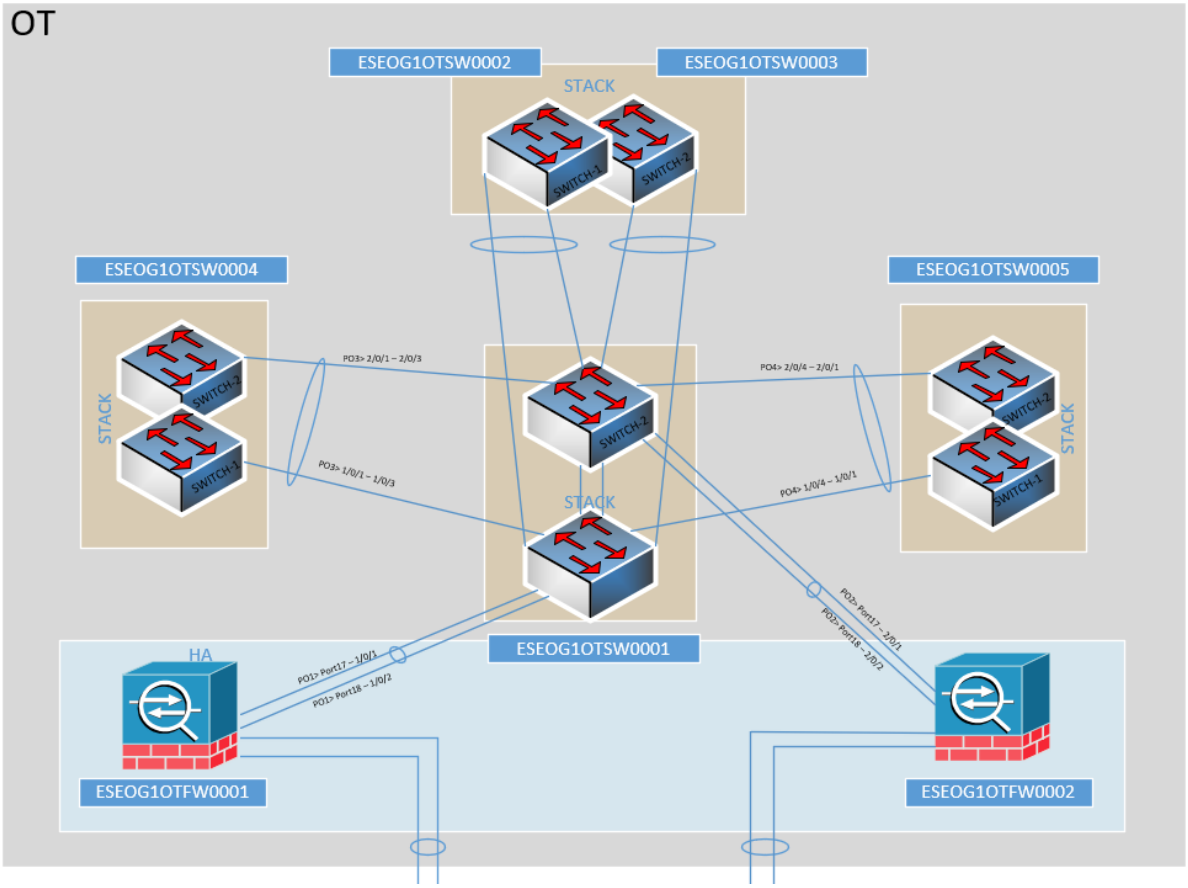
En aquesta taula es mostren els dispositius de xarxa amb la seva nomenclatura i configuració

IP:

ID Actiu	Tipus	Descripció	IP gestió
ESEOG1OTFW0001	Firewall	Firewall FG201F 1	10.14.160.1
ESEOG1OTFW0002	Firewall	Firewall FG201F 2	
ESEOG1OTSW0001	Switch	Switch core 9300X(stack de 2 switches)	10.14.160.3
ESEOG1OTSW0002	Switch	Switch TOR S4112F	10.14.160.4
ESEOG1OTSW0003	Switch	Switch TOR S4112F	10.14.160.5

ESEOG1OTSW0004	Switch	Switch acceso 9200L (stack de 3 switches)	10.14.160.6
ESEOG1OTSW0005	Switch	Switch acceso 9200L (stack de 2 switches)	10.14.160.7
ESEOG1OTSW0006	Switch	Switch acceso 9200L spare	10.14.160.8

3.2.4 Diagrama físic de xarxa



3.3 DISSENY LÒGIC DE LA XARXA

3.3.1 Topologia

- **Xarxa d'agregació:**

  S'anomena xarxa d'agregació aquella xarxa que s'utilitza per interconnectar els dispositius entre xarxes d'accés i xarxes de serveis, amb l'objectiu de commutar i encaminar de manera fiable el trànsit de xarxa.

  La xarxa d'agregació es configura amb el protocol PVRSTP per reduir el temps de convergència quan passa un canvi a la topologia per VLAN. Els switches core seran aquells que enllacen amb els switches d'accés i es configuren amb interfícies

lògiques administrades per la tecnologia EtherChannel, també conegudes com a Link Aggregation Group (LAG), amb l'objectiu de combinar l'amplada de banda de diversos ports Ethernet en un sol enllaç lògic fent coincidir les interfícies del Channel Group a cadascun dels switches involucrats. Aquestes interfícies es configuren com a interfícies de Capa 2 i membres de VLAN.

Cada switch core disposarà de diverses interfícies d'agregat per a la connexió amb els switchs d'accés, firewalls i entorn de màquines virtuals.

En tots els casos, la capa 3 queda configurada als firewalls, els quals estan configurats en mode clúster actiu/passiu, representant de manera abstracta múltiples interfícies que actuen com un únic grup, amb l'objectiu d'augmentar la disponibilitat en cas de fallada i la confiança dels encaminaments a través duna selecció automàtica d'un router virtual.

- **Xarxa d'accés:**
  Les xarxes d'accés de cada entorn exerceixen funcions de nivell 2 i es configuren amb el protocol LACP amb loop detection, amb lobjectiu d'augmentar la disponibilitat de la xarxa i garantir una comunicació sense bucles. Els LACP els tanquen els dos switches core per monitoritzar i controlar cada àrea d'accés respecte als errors de la xarxa, un dels quals és el switch màster i enviant trames de prova des de tots els ports per evitar bucles.

3.3.2 Tipus de xarxes

- **Transit:**
  Una xarxa de trànsit és una VLAN que transporta trànsit en trànsit, és a dir, trànsit que no té l'origen o la destinació final en aquesta VLAN. Per exemple, les VLANs que interconnecten els tallafocs d'IT amb els tallafocs d'OT.

- **DMZ:**
  És la xarxa perimetral que dóna connectivitat a dispositius i/o serveis exposats a xarxes externes de risc, i alhora a xarxes de serveis.

- **Serveis:**
  Capa de xarxa que dona connectivitat a màquines virtuals i dispositius de servei exposats a les diferents xarxes d'accés.

- **Accés:**
  Nivell més baix de xarxa, l'objectiu del qual és donar connectivitat a usuaris, endpoints i dispositius finals.

3.3.3 Definició de les VLAN's

- **VLAN globals:**

Es defineixen com a VLANs globals aquelles VLANs que es propaguen entre IT i OT, per tal d'estendre una VLAN entre més d'un entorn.

Es reserven els identificadors de VLANs globals des del 20 fins al 99. Aquests no es poden repetir a l'entorn IT/OT.

- **VLAN serveis:**
  Es defineixen com a VLANs de serveis, aquelles VLANs l'ús de les quals està reservat per a la gestió dels serveis de xarxa i les xarxes de màquines virtuals. La comunicació dels serveis queda restringida a:
  - Serveis d'autenticació
  - Serveis d'administració indispensables ○ Accés específic a usuaris i dispositius a operar i/o mantenir.

    Es reserven els identificadors de VLANs des de 100 fins a 299.

- **VLAN accés:**
  Es defineixen com a VLANs d'accés a aquelles VLANs la propagació dels quals es limita a xarxes d'usuaris i dispositius a l'entorn IT i dispositius industrials a l'entorn OT.

  Es reserven els identificadors de VLANs des de la 300 en endavant.

3.3.4 Tipus de firewalls

- **Firewalls IT:**
  Segmenta les xarxes de MV, usuaris, dispositius i serveis d'IT, així com la interconnexió amb xarxes corporatives d'altres centres o Internet. Aquest tallafoc segmenta el trànsit a nivell 4 i 7.

  El firewall d'IT és l'únic punt d'entrada a les xarxes de la companyia i l'únic enllaç amb les xarxes industrials a través de la VLAN de trànsit amb el Firewall d'OT.

- **Firewall OT:**
  Segmenta les MV que comuniquen amb els dispositius i servei instal·lats a la DMZ Industrial, xarxes de MV internes i xarxes de control de processos. Aquest tallafoc segmenta el trànsit a nivell 4 i 7.

  El firewall d'OT és l'únic punt d'entrada i sortida de la xarxa d'OT, a través del vostre VLAN de trànsit amb el Firewall d'IT.

3.3.5 Segmentació de xarxa

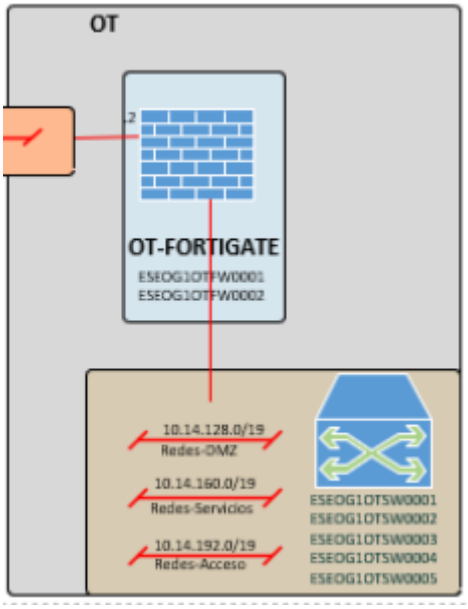
La segmentació de la xarxa és una contra mesurà de seguretat que cal aplicar, complementària a altres contramesures, per reduir el risc associat amb els actius. La

segmentació és el punt de partida on sustentar l'aplicació de les diferents polítiques de ciberseguretat d'acord amb el nivell de risc.

En la següent taula s'exposen el principis de la segmentació:

Principi	Descripció
Grandària de subxarxes	Una subxarxa ha de tenir la mida adequada per adaptar-se al nombre d'actius a segmentar. Exemple: Els sistemes que requereixen un nombre reduït d'adreces IP no s'han d'agrupar en una subxarxa sobredimensionada.
Agrupació d'actius per criticitat	Agrupar els sistemes en les mateixes VLAN/subxarxa si suporten el mateix procés, i si la pèrdua de disponibilitat d'un sistema/actiu afecta la continuïtat de tot el procés.
Agrupació d'actius amb necessitat de comunicació amb altres subxarxes	Segmentar els actius/sistemes amb necessitats similars de comunicació amb altres subxarxes per bloquejar la possible propagació d'un incident de seguretat i limitar els intents de moviments laterals.
Segmentació de servidors de bases de dades	Segmentar els servidors de bases de dades a subxarxes de seguretat separades. Nota: Si el servidor de la base de dades només s'utilitza per a un procés concret, no cal que estigui en una subxarxa separada, pot estar en una mateixa VLAN amb altres sistemes del mateix procés. Exemple: SQL, històrian, servidor OPC que recull dades de múltiples sistemes.

3.3.6 Diagrama lògic de xarxa



4 INFRAESTRUCTURA VIRTUAL HIPERCONVERGENT

4.1 INTRODUCCIÓ

4.1.1 Visio general

El departament d'Automatització està sota un programa de treball i transformació cap a una infraestructura hiperconvergent (HCI) per alinear la tecnologia amb els pilars estratègics.

Una infraestructura HCI és un sistema unificat i definit per programari que aplega tots els elements d'un centre de dades tradicional: emmagatzematge, recursos de còmput, xarxa i gestió. Aquesta solució integrada utilitza programari i servidors per substituir les solucions convencionals amb cabines de discos, reduint la complexitat del centre de dades i incrementant-ne l'escalabilitat.

Principals avantatges de l'arquitectura instal·lada:

- Solució hiperconvergent dissenyada per a entorns crítics, essent l'únic appliance del mercat que aporta una enginyeria i suport conjunt fins a la capa de virtualització.
- Supervisió unificada des d'una única consola, en lloc de gestionar els hosts i emmagatzematge per separat.
- Solució extrem a extrem gràcies a la completa integració entre el maquinari i la plataforma de virtualització.
- Possibilitat de barrejar diferents maquinaris en un mateix clúster, evitant caure en un estat d'obsolescència.
- Cada node col·labora amb la resta per integrar-se en una unitat funcional compartint els recursos físics de què disposa, cosa que permet a l'entorn un escalat transparent en còmput, xarxa i emmagatzematge a través de l'agregació de nous nodes.

Els objectius són establir un conjunt d'estàndards globals per a l'arquitectura, la tecnologia i les operacions OT implementant un disseny basat en les arquitectures de referència estàndard i les bones pràctiques de VxRail.

S'ha implementat la nova infraestructura seguint els principis d'arquitectura:

- **Simple/Estandaritzat**: Redueix la complexitat del disseny gràcies a l'elecció acurada de tecnologies complementàries perquè tant el desplegament com el manteniment posterior sigui fàcilment gestionable i escalable.
- **Disponibilitat**: Mantenir alts nivells de disponibilitat dels serveis crítics.
  Es tindran en compte els següents axiomes:
    - La solució està dissenyada per poder recuperar-se duna fallada de component físic.
    - La solució evita punts únics de fallada.
    - L'arquitectura ha de permetre/facilitar el failover d'un site o serveis del CPD primari a un CPD de DR futur.

- **Flexible/Escalable/Elàstica**: La plataforma és modular i escalable, de manera que el servei permet acomodar creixement futur, tant planificat com no planificat.
- **Virtual Per Defecte**: Per capitalitzar els beneficis de cost i gestió d'un entorn virtual, totes les càrregues de treball haurien de ser virtualitzades dins de la nova infraestructura, llevat que hi hagi raons tècniques o de negoci que el desaconsellin.
- **Segura Per Disseny**: Aquesta plataforma hauria de ser Segura per disseny, i complir o excedir els requeriments funcionals de seguretat traslladats pel client . S'aplica focus específic en la segregació dels fluxos de dades entre els diferents dominis de seguretat

En conclusió, aquest disseny està basat en les arquitectures de referència i les Best practices tant de Dell com de VMWare, que han estat adaptades per complir els requeriments funcionals i de servei de l'empresa.

4.2 GENERALITATS DE L'ENTORN

4.2.1 Solució hiperconvergent VxRail Dell

La solució hiperconvergent VxRail és una plataforma d'infraestructura convergent dissenyada per oferir una solució integrada, escalable i fàcil d'administrar per a càrregues de treball de virtualització. VxRail és una solució de maquinari i programari que combina servidors, emmagatzematge i xarxes en una única plataforma per proporcionar una infraestructura completa per a centres de dades empresarials.

És l'únic dispositiu hiperconversor desenvolupat específicament i totalment optimitzat, creat i dissenyat conjuntament amb VMware, impulsat pels processadors Intel Xeon. Aquesta solució d'hiperconvergència permet enfocar-se als factors de transformació TI que fan una empresa més competitiva. La implementació és ràpida, ja que és l'única família del mercat de dispositius d'infraestructura hiperconvergent (HCI) de VMware completament integrada, preconfigurada i prèviament provada.

L'arquitectura dels dispositius VxRail consisteix en nodes modulars, a més de models basats en servidors Dell PowerEdge i VMware Virtual SAN. Permet començar amb 3 nodes i créixer fins a 64. Això ofereix un enfocament predictible de “pagament a mesura que creix”, per a l'escalament vertical i horitzontal futur, conforme evolucionen els requisits del negoci dels usuaris sense planificació anticipadament.

Ofereixen una flexibilitat de configuració extrema que permet escollir el rendiment, la capacitat i la funcionalitat gràfica necessaris per complir els requisits d'infraestructura, amb opcions basades en els servidors PowerEdge.

La solució VxRail també utilitza VMware vSphere per a la virtualització de servidors, cosa que permet que múltiples sistemes operatius i aplicacions s'executin en un sol servidor físic. La solució VxRail es pot administrar mitjançant una única consola d'administració, cosa que simplifica la gestió i permet als administradors de TI implementar i administrar càrregues de treball de manera ràpida i eficient.

Característiques principals dels dispositius VxRail

- Consolidació de càlcul, emmagatzematge, virtualització i administració.
- Rendiment i eficiència, amb la integració de la capa kernel entre el VMware i l'hipervisor vSphere.
- Escala linealment de 3 a 64 nodes, donant suport des de 40 a centenars de VMs.
- Inclou rèplica de dades, còpia de seguretat i desbordament al núvol.
- Ofereix serveis de dades empresarials, resiliència i qualitat de servei.
- Proporciona un punt únic de suport per a programari i maquinari de dispositius.

4.2.2 Infraestructura instal·lada

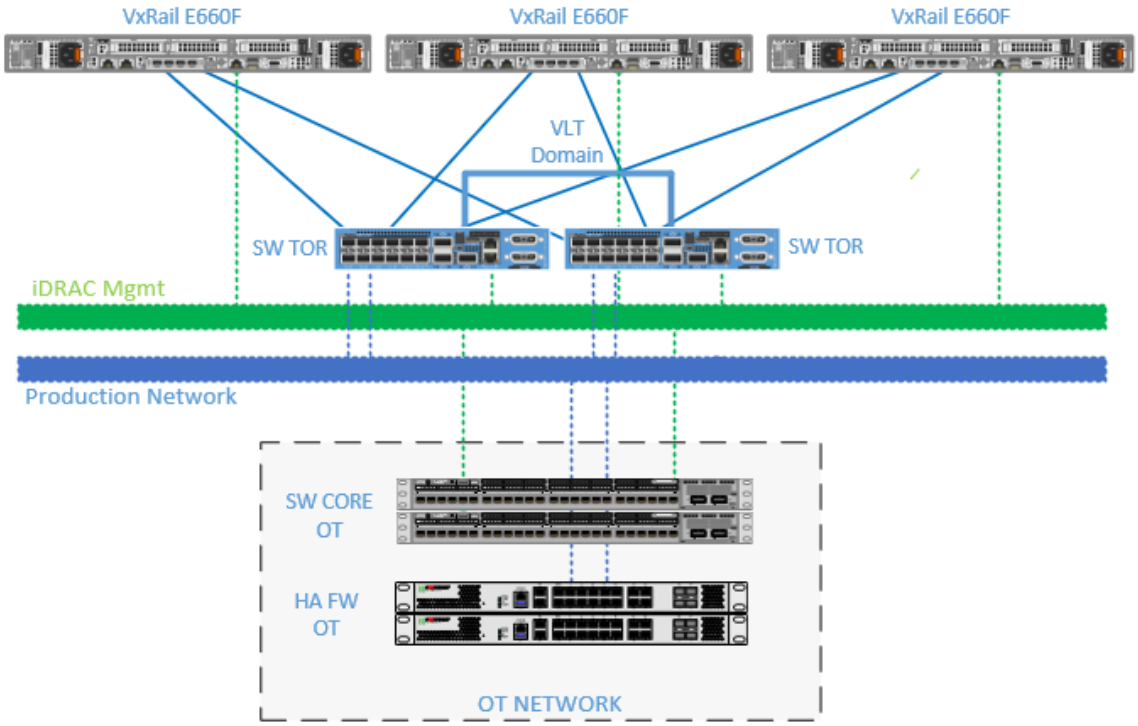
La plataforma hiperconvergent VxRail instal·lada al rack 1 del CPD, inclou infraestructura de xarxa (Top of Rack switches) i nodes VxRail (3) per poder oferir, en 4 RU's, computació, emmagatzematge i xarxa per allotjar les màquines virtuals descrites al punt anterior i la seva producció.

Switches de xarxa ToR
La solució de xarxa física està composta per dos switches Top of Rack del fabricant Dell Technologies, model S4112F-ON. Ambdues unitats, configurades com a clúster VLT, proveeixen serveis de xarxa per poder crear el clúster de VxRail i interconnectar l'entorn hiperconvergent amb els diferents entorns de xarxa del client de forma independent.
En capítols posteriors descriurem la funcionalitat i la configuració d'aquests equips.

Nodes de VxRail
La solució VxRail està composta per 3 nodes de tipus E (model E660F, all-flash). Aquests nodes ofereixen els recursos de computació, emmagatzematge i virtualització per allotjar la producció de la fabrica.

La infraestructura està composta per un clúster hiperconvergent format per 3 nodes VxRail, amb el propòsit d'allotjar totes les màquines virtuals descrites al punt anterior.

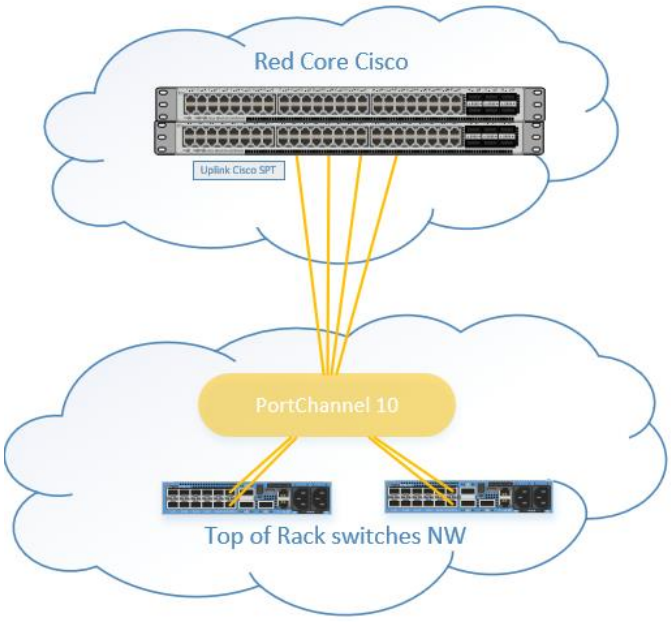
Per a la connectivitat amb les xarxes existents, s'han instal·lat 2 switches TOR (Top Of the Rack) addicionals, la funcionalitat i configuració de les quals es descriu en els capítols posteriors.



Tots els components de la infraestructura instal·lada estan previstos de maquinari redundant per no tenir punts únics de fallada.

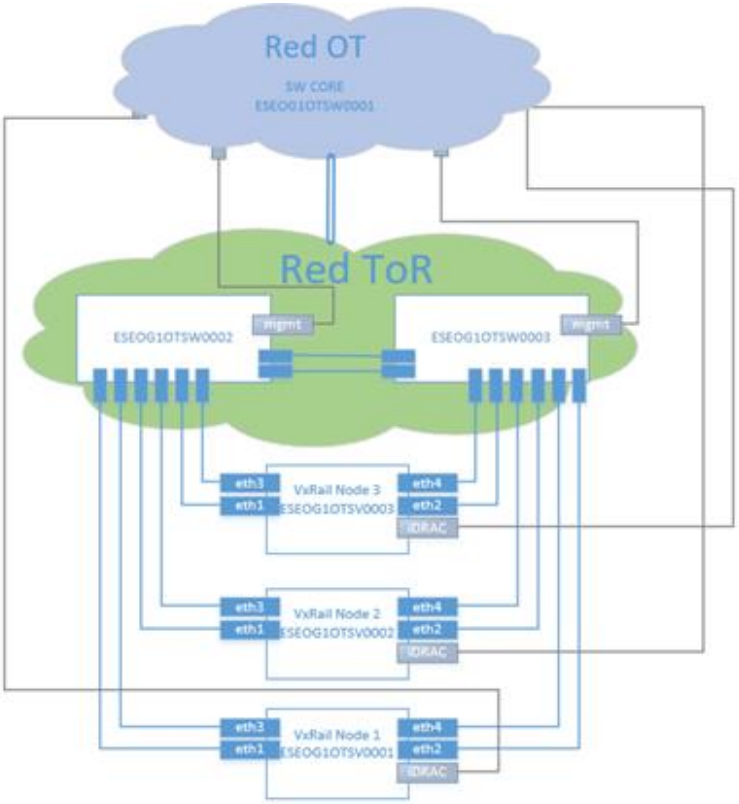
4.3 CONFIGURACIÓ DE XARXA

L'arquitectura configurada cobreix els components físics, així com les configuracions respectives per poder integrar i donar suport a la infraestructura VxRail, d'acord amb els requisits de la solució i les bones pràctiques recomanades tant per Dell Technologies com per VMware en entorns similars.



En aquesta topologia, cadascun dels nodes de VxRail té la meitat dels seus ports connectats a cada switch, seguint les best practices de Dell Technologies per a entorns d'aquest tipus.

A continuació, es mostra el diagrama de connectivitat a alt nivell:



4.3.1 Configuració switchos TOR

La xarxa TOR per al clúster VxRail compleix els punts següents:

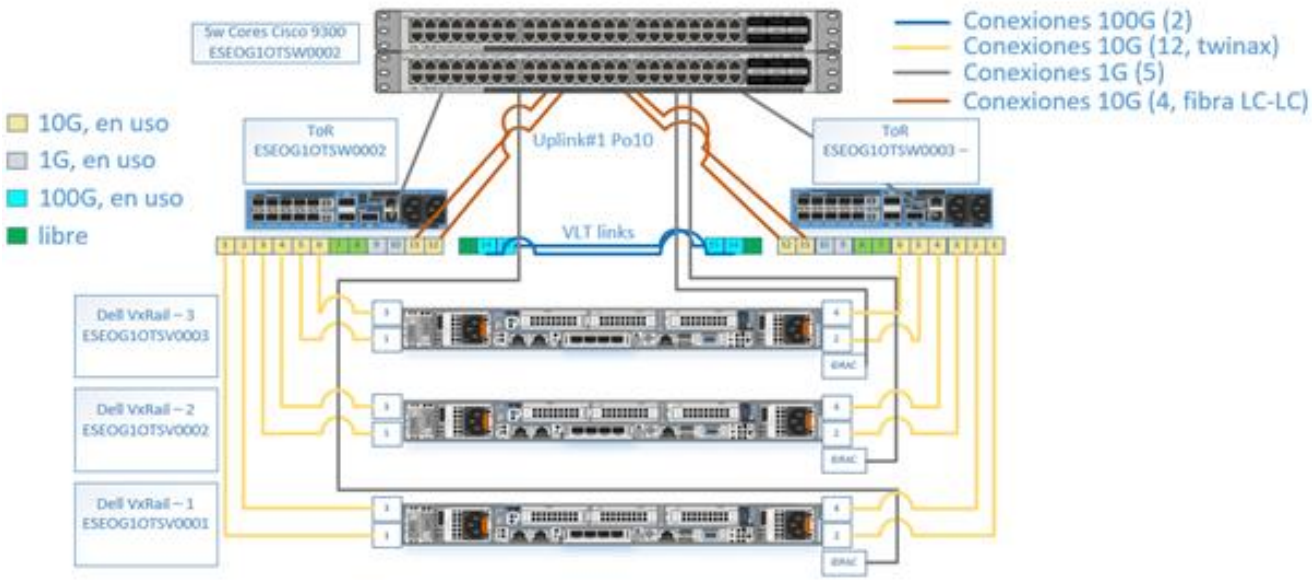
- S'estableix un clúster VLT entre tots dos switches, interconnectats amb 2 interfícies de 100GbE per intercanviar informació d'estat i per propagar el trànsit entre els switches, i les dues interfícies de gestió fora de banda per a keepalive.
- Es defineixen totes les VLANs als 2 switches TOR.
- Totes VLANs estan assignades a tots els nodes VxRail per a la comunicació de les VMs a qualsevol de les xarxes.
- Addicionalment a aquestes VLANs, s'han creat VLANs internes als TOR per a funcionament intern, sense estendre's a cap de les xarxes d'OT de la planta industrial.
- Xarxes internes de VxRail
    - Internal Management (keepalive, node Discovery, etc.)
    - vSAN
    - vMotion

En capítols posteriors, es detalla el número de VLAN i la descripció.

Connexions físiques:

- Les connexions físiques entre els nodes VxRail i els switches ToR es realitzen a través de cables TwinAx de 10GbE (12 cables en total).
- Les connexions d'uplink entre els ToR i els switches CORE d'OT de la planta es realitzen a través de SFP's 10G-BaseSR i fibres LC-LC multimode.
- Les connexions VLT es fan utilitzant cables TwinAx de 100GbE.
- Les connexions de gestió fora de banda es realitzen mitjançant cablatge RJ-45, GbE.
- Per a la infraestructura VxRail s'estableixen les VLANs i les característiques següents:
    - La xarxa de gestió interna es configura com a VLAN 107 per a la total automatització en la tasca d'addició de nous nodes.
    - La xarxa de gestió externa s'assigna de manera untagged als nodes VxRail per permetre l'agregació de futurs nodes de forma desatesa.
    - La VLAN 107 té habilitat el multicast per permetre la distribució d'informació via multicast IPv6 entre els nodes del clúster.

A continuació es mostra la topologia detallada de connexió implantada:



Com es pot veure, les connexions imparells de cadascun dels nodes VxRail (ports 1, 3) es connecten al ToR #1 ESEOG1OTSW0001 (esq.), mentre que les parells (ports 2, 4) es connecten al ToR #2 ESEOG1OTSW0002 (dreta). Això respon a com classifica el trànsit el VxRail, i que es descriurà en seccions posteriors.

A la següent taula està definit el nom del switch, model, ip i la ubicació física dins del CPD:

Equip	Nom Switch	IP	Model
TOR	ESEOG1OTSW0001	10.14.160.4	S4112F-ON
TOR	ESEOG1OTSW0002	10.14.160.5	S4112F-ON

Configuració NTP:

Es configura el switch perquè el servei NTP sincronitzi contra el servidor de domini (*La configuració del controladors de domini no es contempla en aquest TFG).

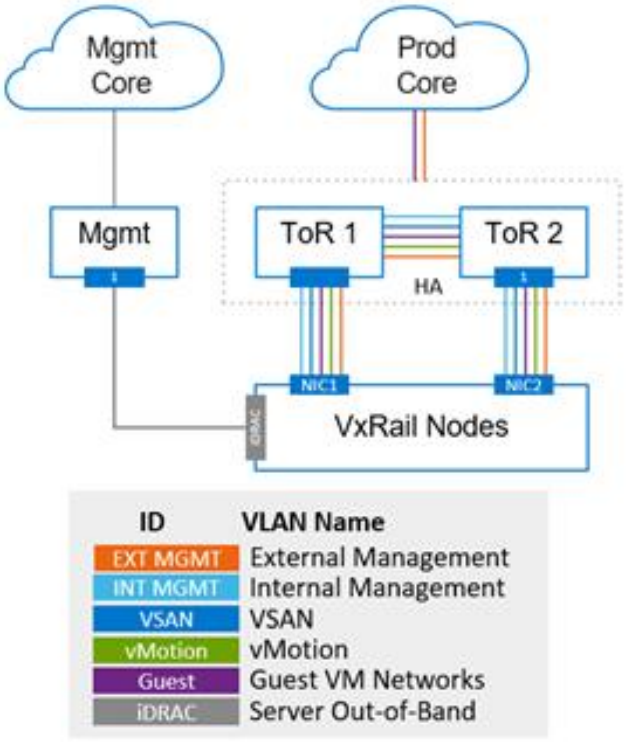
Configuració VLAN's:

Non VLAN	VLAN ID	Xarxa Trunk
ESEOG1OTVL0100	100	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0101	101	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0102	102	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0103	103	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0104	104	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0105	105	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0106	106	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0107	107	VMware HCIA Dist-DVUplinks-12
ESEOG1OTVL0109	109	VMware HCIA Dist-DVUplinks-12

Com es pot apreciar a la taula anterior, aquestes VLANs es poden agrupar en els grans grups següents:

- Xarxes internes per al VxRail (en blau – vMotion, vSAN, internal Management)
- Xarxes de servei usuaris (blanc –Guest VM Networks, external Management, iDRAC)

A continuació, un esquema de la topologia lògica de connexió de xarxa de VxRail:



4.4 CONFIGURACIÓ DEL CLUSTES VXRAIL

S'ha instal·lat un clúster de VxRail estàndard versió 7, compost per 3 nodes amb ESXi versió 7 i gestionat per un vCenter versió 7.

A la taula següent es resumeixen les principals opcions de disseny adoptades i configurades al clúster de VxRail:

Opcio de disseny	Decisio de disseny	Descripcio
Localizacio vCenter	vCenter intern	La plataforma HCI és autocontinguda, de manera que no hi ha elements externs per a la seva administració. A més, el procés d'actualitzacions s'ocupa no només de microprogramari, drivers, BIOS o paquets SW, sinó també de vCenter, Servei de Suport Remot de Dell (SRS) i VxRail Manager. Per a més informació, consulteu el capítol 4.8.2.
Tipus de desplegament	4x10GbE	Quan els nodes de VxRail compten amb targetes NDC de quàdruple port, és possible desplegar sobre 2 d'aquestes interfícies o sobre 4.

		Es realitza el desplegament cap a les 4 per maximitzar la utilització dels recursos de xarxa.
Deduplicacio i compresio	No s'habilitarà deduplicació ni compressió a la vSAN	En sistemes All-Flash, vSAN permet habilitar aquesta característica, de manera que s'aplica compressió i deduplicació, oferint un espai útil més gran a la vSAN a costa d'una utilització inicial per als punters de deduplicació i una penalització en consum de CPU.
Versió VxRail	S'instal·la la versió 7.0.370	En el moment del desplegament, la 7.0.370 era la darrera versió disponible que, sent de la família 7.0.x, incloïa els últims fixes de seguretat.
Polítiques d'emmagatzematge	Default vSAN policy: RAID1.	Amb 3 nodes, Només es poden crear polítiques d'emmagatzematge Raid 1, complint amb una tolerància a fallades FTT = 1, permeten optimitzar l'ús de recursos de vSAN (mirror – 2x;).
Logging	Desplegament de VMware LogInsight	Es desplega la solució propietària de VMware per a la gestió de logs vRealize LogInsight.
Connexions a internet	Sense connexió a l'exterior (Dark Site)	Aquesta instal·lació és un dark site, el que significa que cap dels elements té accés a internet (no es pot desplegar SRS, el VxRail manager no es pot descarregar el nou codi, el vCenter no té accés a vmware.com per refrescar HCL o altre tipus d'informació (vSAN).
Enrascarat de nodes – ordenat per número de sèrie	S'ha optat per enrackat ascendent	Com a resultat d'aquesta decisió, el node número u serà el de la posició inferior, mentre que el més nou al clúster estarà sempre a la part superior.

A la taula següent especifiquem les versions del sistema VxRail.

Versión vCenter	7.0.3 build-19480866	***Versión ESXi***	7.0.3- 19482537

4.4.1 Components del clúster

Node Nº	Nom del node	Posició en el rack
1	ESEOG1OTSV0001	1
2	ESEOG1OTSV0002	2
3	ESEOG1OTSV0003	.3

4.4.2 Configuració DNS

Per a la configuració DNS de sistema VxRail es configurarà mitjançant dos servidors DNS (*aquets servidors no es contemplen en aquest TFG), proporcionat així redundància en el sistema de resolució de noms.

Servidors DNS	
Primari	10.14.132.10
Secundari	10.14.132.11

Al DNS del domini s'ha creat els registres DNS (forward i reverse) dels servidors del entorn VxRail.

4.4.3 Configuració NTP

Es configura el sistema perquè el servei de sincronització horària NTP sincronitzi amb el servidor 10.14.132.13.

4.5 CONFIGURACIÓ DE LES INTERFÍCIES

4.5.1 Configuració interfícies físiques iDRAC

iDRAC són les sigles de Dell Remote Access Controller. És un dispositiu de maquinari integrat als servidors que té el seu propi processador, memòria, interfície de xarxa i accés al bus del sistema. iDRAC proporciona accés als nodes de VxRail per gestionar el sistema de forma remota a través de HTTPS. Aquesta connexió ofereix als administradors un punt d'accés als nodes per veure l'estat dels seus components, i també ofereix una interfície

KVM (keyboard, vídeo, monitor) virtual simplificant l'accés remot al servidor a un nivell que és similar a l'accés a la consola del servidor local al centre de dades.

Els 3 nodes tenen una interfície física de xarxa per a la gestió integral del servidor.

Nodo	Direcció IP	Mascara de Xarxa	Porta d'enllaç	Usuari Local	Accés
ESEOG1OTSV0001	10.14.163.10	255.255.255.0	10.14.163.1	root	Web https
ESEOG1OTSV0002	10.14.163.11	255.255.255.0	10.14.163.1	root	Web https
ESEOG1OTSV0003	10.14.163.12	255.255.255.0	10.14.163.1	root	Web https

4.5.2 Configuració interfícies ESXi per a la gestió

La interfície de gestió d'un ESXi és una eina proporcionada per VMware que permet administrar i controlar servidors ESXi, que són hipervisors utilitzats per virtualitzar sistemes operatius. Aquesta interfície, generalment accessible a través d'un navegador web, ofereix funcions per configurar i supervisar els recursos dels servidors virtuals, com crear i gestionar màquines virtuals, assignar recursos de CPU i memòria, establir polítiques d'emmagatzematge i xarxes, així com monitoritzar el rendiment i rebre alertes d'esdeveniments. La interfície de gestió ESXi proporciona una manera convenient d'administrar i mantenir un entorn virtualitzat de manera eficient.

A les taules següents especifiquem els paràmetres virtuals configurats a les interfícies ethernet de l'entorn.

Nodo	Direcció IP	Mascara de Red	Porta d'enllaç	Usuari Local	Accés
ESEOG1OTSV0001	10.14.162.10	255.255.255.192	10.14.162.1	root	Web https
ESEOG1OTSV0002	10.14.162.11	255.255.255.192	10.14.162.1	root	Web https
ESEOG1OTSV0003	10.14.162.13	255.255.255.192	10.14.162.1	root	Web https

4.5.3 Configuració interfícies vSAN

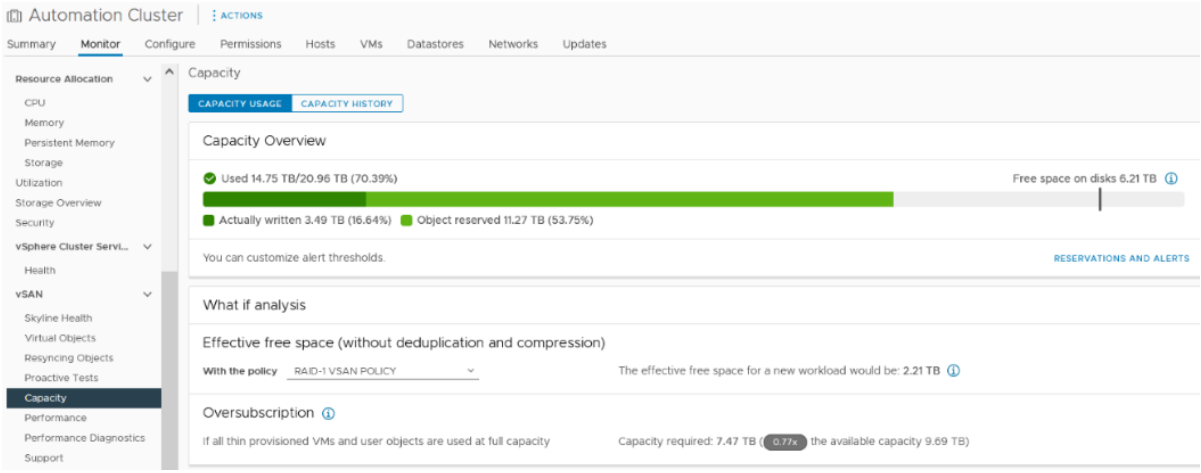
vSAN (Virtual SAN) és la solució de VMware que permet crear un entorn d'emmagatzematge definit per programari (SDDC) en un clúster ESX. VxRail adopta aquesta tecnologia i gràcies a la col·laboració de les enginyeries de Dell Technologies i VMware, VxRail és l'única solució hiperconvergent basada en ESX que optimitza HW i SW per donar les millors prestacions del mercat.

vSAN utilitza la tecnologia d'hipervisor per distribuir i replicar les dades a través de múltiples nodes del clúster, proporcionant redundància i tolerància a errors sense necessitat d'una xarxa d'emmagatzematge externa. Alguns dels avantatges clau de vSAN són:

- **Simplificació de la infraestructura:** vSAN elimina la necessitat dun emmagatzematge extern i costós, reduint la complexitat i les despeses generals de la infraestructura.
- **Escalabilitat:** Permet escalar fàcilment l'emmagatzematge mitjançant l'addició de nous nodes al clúster. Els recursos d'emmagatzematge s'afegeixen i s'utilitzen de manera eficient a mesura que creix l'entorn.
- **Alta disponibilitat i tolerància a errors:** vSAN replica les dades a través de múltiples nodes, cosa que garanteix la disponibilitat de les dades fins i tot en cas de fallada d'un node o disc.
- **Rendiment optimitzat:** Mitjançant l'ús de SSD i tècniques de memòria cau intel·ligents, vSAN ofereix un rendiment superior i una latència reduïda per a les càrregues de treball virtualitzades.
- **Integració nativa amb VMware:** vSAN s'integra perfectament amb l'stack de virtualització de VMware, cosa que en facilita la implementació i la gestió a través de les mateixes eines i interfícies utilitzades per administrar les màquines virtuals.
- **Administració centralitzada:** vSAN s'administra mitjançant una interfície de gestió intuïtiva que permet configurar i monitoritzar l'emmagatzematge de manera centralitzada, simplificant les tasques d'administració i de troubleshooting.
- **Eficiència en el consum de recursos:** vSAN utilitza tècniques avançades de deduplicació i compressió de dades, cosa que redueix l'empremta d'emmagatzematge i optimitza l'ús dels recursos.

La vSAN es crea automàticament juntament amb el clúster VxRail. Amb la distribució de discos per host proveïda (cada node compta amb 2 disk-groups composts cadascun per un disc de memòria cau de 400Gb i 4 discos de capacitat de 1.9TB SSD), la capacitat total bruta de la vSAN és de 20,96 TB.

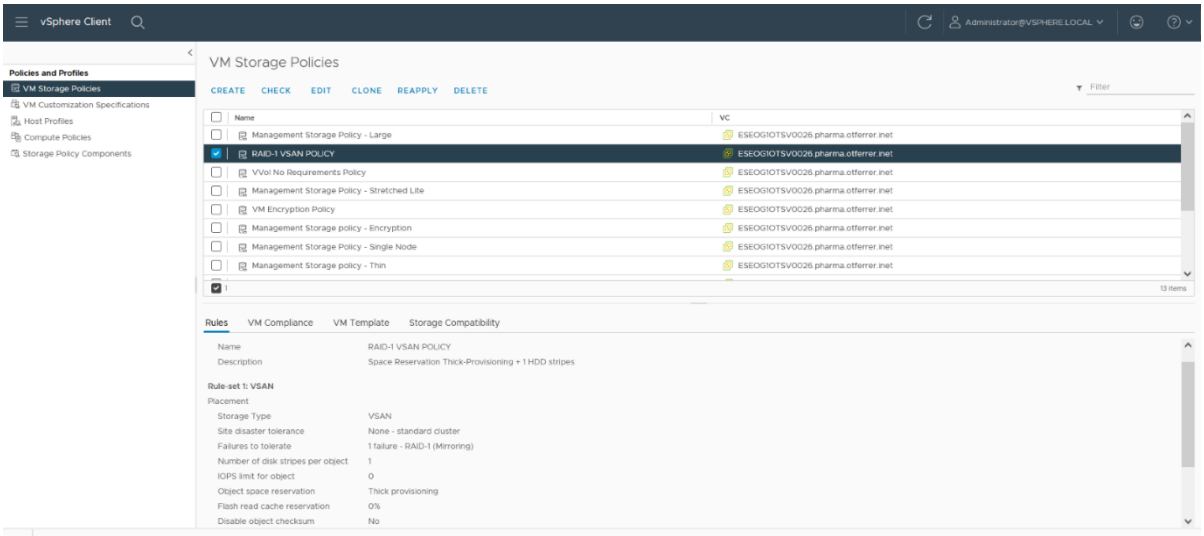
En la següent imatge podem visualitzar la capacitat del clúster VxRail:



Al clúster de 3 nodes de la infraestructura es configuren la següent política de protecció de dades:

- Protecció RAID-1 VSAN Policy.

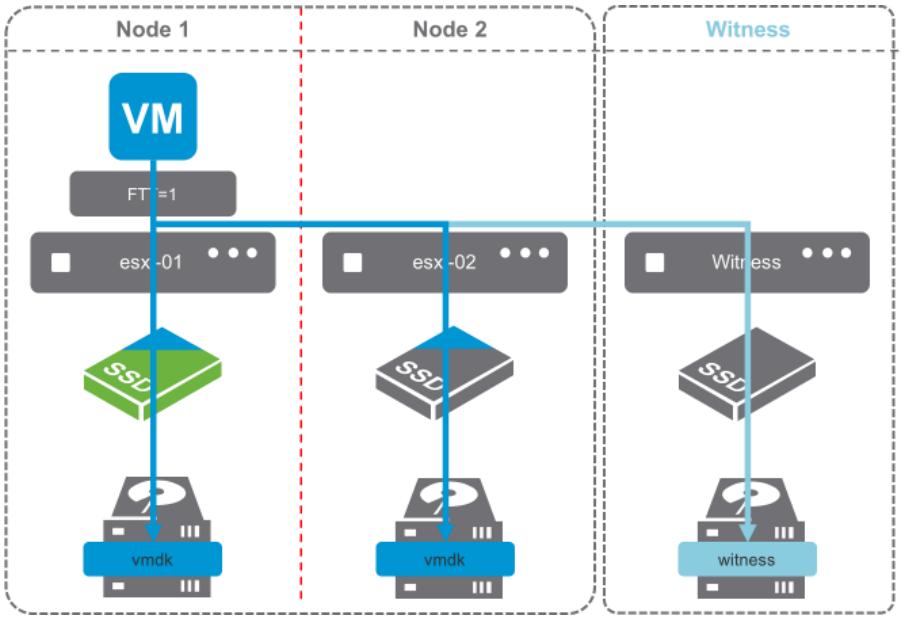
Per defecte, es configura la política de protecció de dades per emmagatzemar les MV en format thick i protecció RAID1. A la imatge següent observem la política d'emmagatzematge creada:



Configurem per defecte de la política d'emmagatzematge “RAID-1 VSAN Policy” al datastore d'AUT-DATASTORE-01.

Com a principals característiques:

- RAID-1 VSAN Policy.: consumeix el doble d'espai a vSAN de la capacitat a guardar, però ofereix el millor rendiment
- Aquesta serà la política d'emmagatzematge per defecte, de manera que, si desplegueu una nova VM no s'especifica res, en aquest clúster aquesta VM tindrà assignada la política Raid-1 VSAN Policy:



Addicionalment, vSAN ens permet les següents característiques:

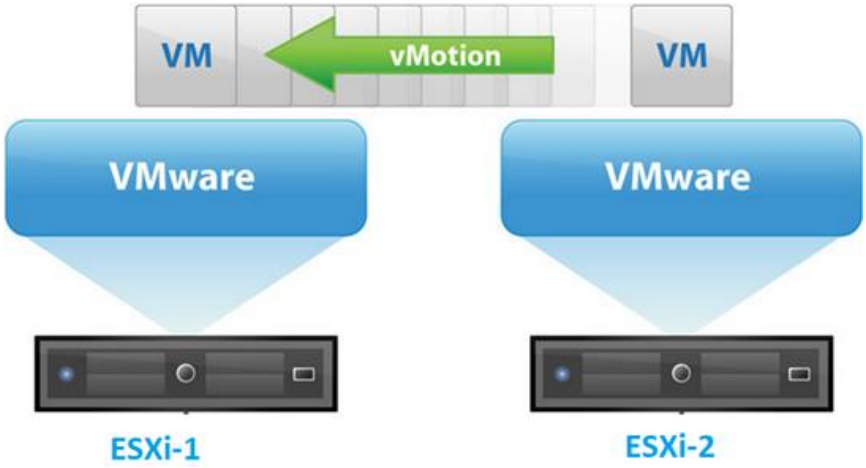
- Canvi de polítiques de protecció en calent a les VMs, sense disrupció
- Granularitat d'aplicació de les polítiques: es poden aplicar les polítiques a nivell global per a una VM, o per cadascun dels seus objectes.
- Deduplicació i compressió: permet optimitzar l'espai.

S'ha configurat vSAN amb les característiques de xarxa següents:

vSAN Node	Direcció IP	Mascara de Xarxa	VLAN
ESEOG1OTSV0001	10.14.162.138	255.255.255.192	106
ESEOG1OTSV0002	10.14.162.139	255.255.255.192	106
ESEOG1OTSV0003	10.14.162.140	255.255.255.192	106

4.5.4 Configuració interfícies VMotion

vMotion és una característica de VMware que permet la migració en temps real de màquines virtuals (VMs) en execució d'un servidor físic a un altre sense interrupció de servei perceptible per als usuaris.



Amb vMotion, les VMs es poden moure entre hosts dins d'un clúster de servidors ESXi sense experimentar temps d'inactivitat. Durant la migració, la memòria, l'estat i tots els recursos associats amb la VM es transfereixen sense problemes al nou host, mentre que les connexions de xarxa i l'emmagatzematge es mantenen actius.

La migració vMotion es basa en una infraestructura de xarxa compartida i emmagatzematge compartit entre els amfitrions, cosa que garanteix una connectivitat constant i una continuïtat de servei sense interrupcions.

Els beneficis de vMotion inclouen:

- **Major flexibilitat:** Permet realitzar tasques de manteniment a servidors sense afectar la disponibilitat de les aplicacions en funcionament.
- **Balanceig de càrrega:** Les VMs es poden moure d'un amfitrió sobrecarregat a un amb recursos disponibles, equilibrant la càrrega de treball i optimitzant el rendiment del sistema.
- **Millora de la disponibilitat:** En cas de fallada del maquinari, les VMs es poden migrar automàticament a un host de seguretat, minimitzant el temps d'inactivitat.
- **Migració sense interrupcions:** Els usuaris poden accedir a les aplicacions i serveis sense notar cap interrupció durant la migració.

S'ha configurat una xarxa de VMotion a tots els nodes VxRail per possibilitar la migració en viu de màquines virtuals en execució des d'un servidor físic a un altre sense temps fora de servei, amb disponibilitat constant del servei i una integritat de tota la transacció.

S'ha configurat VMotion amb les característiques següents:

vMotion Nodo	Direcció IP	Mascara de Xarxa	VLAN
ESEOG1OTSV0001	10.14.162.74	255.255.255.192	105
ESEOG1OTSV0002	10.14.162.75	255.255.255.192	105
ESEOG1OTSV0003	10.14.162.76	255.255.255.192	105

4.5.5 Internal Managment

La xarxa de gestió interna es comparteix entre els nodes físics i el VxRail Manager, utilitzant adreces IPv6 autoassignades.

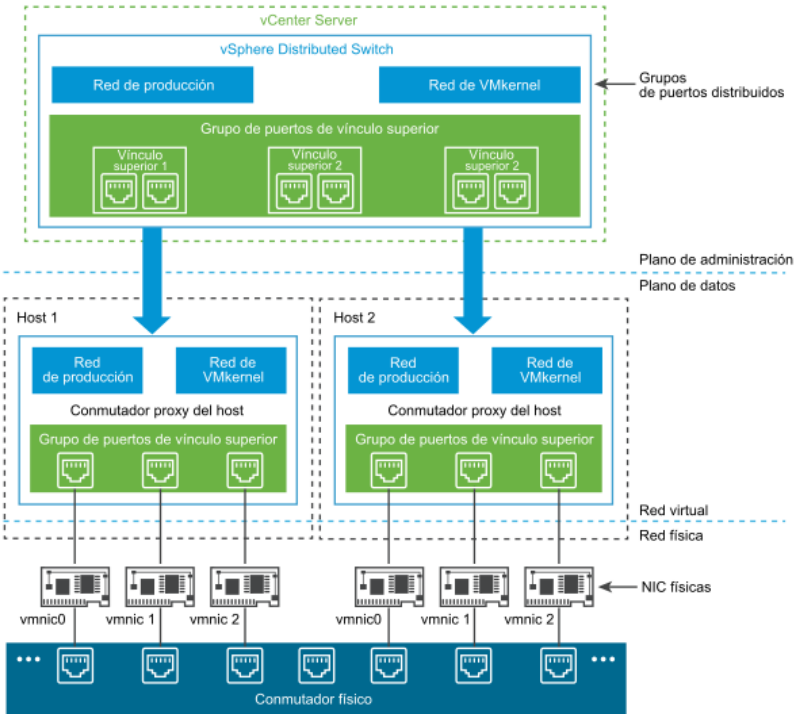
Aquesta xarxa no es propaga a l'entorn de la infraestructura del cluster VxRail, i queda únicament accessible entre els switches TOR i els nodes VxRail. El trànsit generat en aquesta xarxa és multicast, la xarxa que dóna servei a VxRail ha de suportar aquesta funcionalitat habilitant el “MLD snoopong” i “l'IPv6 snooping voler” en aquesta VLAN.

Al desplegament de l'entorn s'ha configurat l'ID de VLAN 107 per a aquesta xarxa.

4.5.6 Configuració VDS Network Portgroups.

VMware vSphere Distributed Switch (VDS) és un component clau de la plataforma de virtualització de VMware vSphere. És una solució de commutador virtual distribuït que permet ladministració centralitzada i simplificada de la connectivitat de xarxa en un entorn virtualitzat.

El VDS es desplega a nivell de clúster i proporciona una única instància de configuració i polítiques de xarxa per a tots els hosts en aquest clúster. Això elimina la necessitat de configurar i administrar els commutadors virtuals a cada host de forma individual.



Algunes de les característiques i avantatges del VDS inclouen:

- **Gestió centralitzada:** Permet la configuració i administració unificada de la xarxa a tots els hosts del clúster, la qual cosa simplifica les tasques d'administració i configuració.
- **Portabilitat i mobilitat de VM:** Permet la migració en calent (vMotion) de màquines virtuals entre hosts sense canviar la configuració de xarxa, cosa que garanteix la continuïtat del servei i simplifica l'administració.
- **Polítiques de xarxa avançades:** Permet l'aplicació de polítiques de xarxa coherents a tots els hosts, com la segmentació de xarxa mitjançant VLANs i la configuració de QoS (Quality of Service).
- **Monitorització i diagnòstic:** Proporciona eines de monitorització i diagnòstic avançades per a la detecció i resolució de problemes de xarxa.

A la taula següent s'especifica les xarxes creades dins del VDS "Virtual Distribute Switch" i que donen servei a tota la infraestructura i entorn:

Tipus	Nom VLAN	VLAN ID
VM	ESEOG1OTVL0100	100
VM	ESEOG1OTVL0101	101
VM	ESEOG1OTVL0102	102
VM	ESEOG1OTVL0103	103

External Management	ESEOG1OTVL0104	104
vCenter Network	ESEOG1OTVL0104 -vCenter Network	104
VMOTION	ESEOG1OTVL0105	105
VSAN	ESEOG1OTVL0106	106
INTERNAL MANAGEMENT	ESEOG1OTVL0107	107

4.6 COMPONENTS DE VXRAIL

4.6.1 VxRail Manager

VxRail Manager és l'element diferenciador d'un cluster VxRail, i les funcions són les següents:

- Automatitzar les més de 300 tasques que comporta el desplegament inicial d'un cluster VxRail
- Descobriment automàtic de nous nodes durant les tasques d'expansió del clúster.
- Simplifica el procés d'addició de discos mitjançant un wizard que, en funció del tipus de discos a afegir (cache, capacitat) ofereix les millors opcions de posicionament dels nous discos, i procedeix amb les expansions dels diferents disk group de cada node per contribuir al creixement de la capacitat de la vSAN.
- Ofereix una vista de l'estat de salut del clúster.
- Automatitza les actualitzacions de codi de VxRail, de manera que el procés total es realitza pràcticament de manera desatesa. Fins i tot en cas que no hi hagi DRS, VxRail Manager ofereix la possibilitat d'assignar una llicència temporal de vSphere Enterprise, amb DRS, que automatitzi la migració de VMs dels hosts per poder reiniciar el cluster node a node sense afectació de servei.

VxRail Manager es veu com un plugin integrat amb el vCenter, a través de les vistes següents:

- Vista VxRail (des del desplegable Menú – VxRail)
- Des de la vista Hosts and Clusters, a l'apartat de Monitorització, secció VxRail (canviarà si se selecciona el clúster o només un dels host). Els submenús disponibles en aquesta secció són:
    - Hosts: ofereix una vista 'física' de cada node, i en cas de fallada de component, ens mostrarà una icona derror o de warning al costat de l'element que està donant la fallada.
    - Last Configuration Data Sent: en cas que SRS (Servei de Suport Remot de Dell) estigués desplegat, ens permet veure quina informació ha intercanviat el clúster amb els sistemes de suport de Dell Tecnologies i el portal ACE (myvxrail.emc.com) . En el nostre cas, com que és un dark site aquest punt no aplica, ja que no denega qualsevol comunicació amb l'exterior.

- Des de la vista Hosts and Clusters, a l'apartat de Configuració, secció VxRail. Els submenús disponibles són els següents:
    - System: ens dóna una vista de quina versió de microprogramari de VxRail tenim desplegada i des de quan.
    - Updates: ens permet engegar el bloc d'actualitzacions.
    - Certificate: en cas que necessiteu aplicar un conjunt de certificats d'usuari per a l'accés al clúster, aquesta és la secció.
    - Market: repositori de les aplicacions disponibles per a VxRail (vRops, RP4VMs, DDVM, Isilon SD, etc.)
    - Add VxRail hosts: permet descobrir els hosts i arrencar el wizard que ajuda en el procés dafegir nous nodes.
    - Hosts: en cas que sigui necessari fer algun procés de canvi de configuració dels nodes, aquest és el punt d'arrencada.
    - Support: Com que és un dark site no aplicaria aquesta secció però des d'aquí es configura l'usuari eSRS, així com la VM de l'SRS (opcional)
    - Networking: ens permet habilitar la xarxa en cas de sortida a Internet, configurar proxy de sortida i la freqüència amb què VxRail Manager actualitza de l'estat al vCenter (throttling)
    - Troubleshooting: per obtenir els logs dels diferents elements (VxRail Manager, vCenter, els hosts ESXi, etc.).

S'ha configurat la Vxrail Manager amb les característiques de xarxa següents:

Nom VxRail Manager	Direcció IP	Màscara	Gateway
ESEOG1OTSV0027	10.14.162.61	255.255.255.192	10.14.162.1

A la taula següent es mostren els valors d'accés a la gestió.

Usuari Root	Usuari de gestió	Accés
Root	Mystic	SSH

4.6.2 vCenter

vCenter Server és una plataforma de gestió centralitzada de VMware que permet administrar i controlar de manera unificada els entorns de virtualització basats en VMware vSphere. És una aplicació de servidor que actua com a centre de control per a la gestió de màquines virtuals, clústers, recursos d'emmagatzematge i xarxes en un entorn vSphere.

Algunes de les funcions clau de vCenter Server inclouen:

- Gestió centralitzada: Proporciona una interfície única per administrar múltiples hosts ESXi i les seves màquines virtuals en un entorn vSphere.

- Aprovisionament i desplegament de VM: Permet crear i desplegar fàcilment noves màquines virtuals, configurant paràmetres com a CPU, memòria, emmagatzematge i xarxes.
- Monitorització i rendiment: Ofereix eines per supervisar el rendiment del clúster, les VM i els recursos de maquinari, generant alertes i ajudant a identificar colls d'ampolla.
- Alta disponibilitat: Facilita la configuració i administració de característiques com vMotion i HA (High Availability), que garanteixen la continuïtat del servei i la recuperació davant de falles.
- Gestió de recursos: Permet l'assignació i el control de recursos de CPU, memòria i emmagatzematge a nivell de clúster i màquina virtual.

S'ha desplegat un VCSA intern per a la gestió de l'entorn virtual de VMWare amb les característiques següents.

- Com que el VCSA forma part del cicle de vida del VxRail, amb cada nova actualització de programari del clúster, el vCenter és actualitzat juntament amb la resta dels elements de forma automàtica i desatesa.
- El vCenter estarà físicament dins del clúster VxRail.
- vCenter ve llicenciat de fàbrica i només pot gestionar el clúster VxRail.

Es realitza el desplegament VCSA dins l'entorn de VxRail per a la gestió centralitzada de l'entorn virtual dels 3 nodes ESXi.

La llicència de VCSA s'inclou amb VxRail en haver realitzat un desplegament intern del servidor vCenter.

S'ha configurat vCenter amb les característiques de xarxa següents.

Nom vCenter Manager	Direcció IP	Màscara	Gateway
ESEOG1OTSV0027	10.14.162.60	255.255.255.192	10.14.162.1

A la taula següent es mostren els valors d'accés a la gestió.

Usuari Administrador	Usuari Management	Accés
administrator@vsphere.local	admin	https:// 10.14.162.60:5480

4.6.2.1 Accesos i privilegis a la infraestructura virtual vCenter

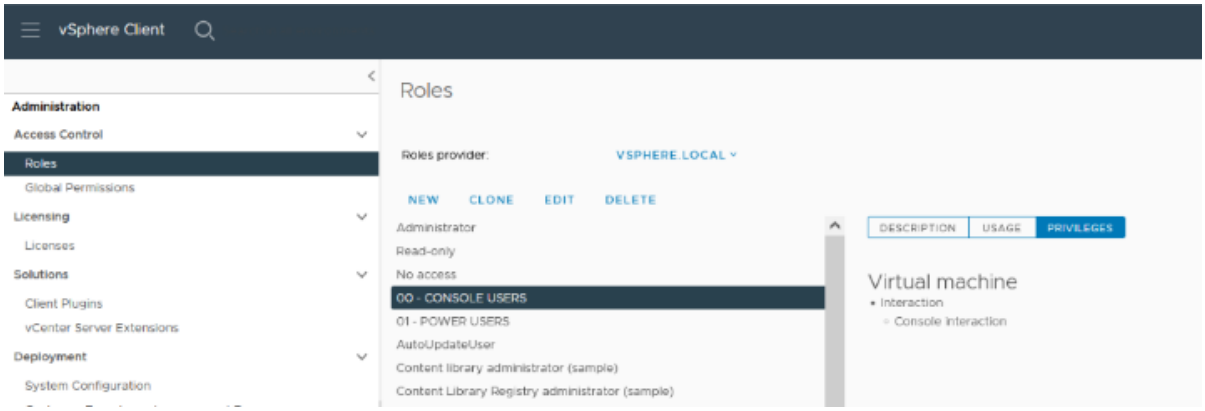
Dins del control d'accessos de la infraestructura virtual, s'han creat dos nous ROLS anomenats “00 – CONSOLE USERS” i “01 – POWER USERS” amb privilegis per poder realitzar les següents accions a les màquines virtuals.

ROL: “00 - CONOLE USERS”

Interaction:

Console interaction

Tal com podem veure a la següent imatge:

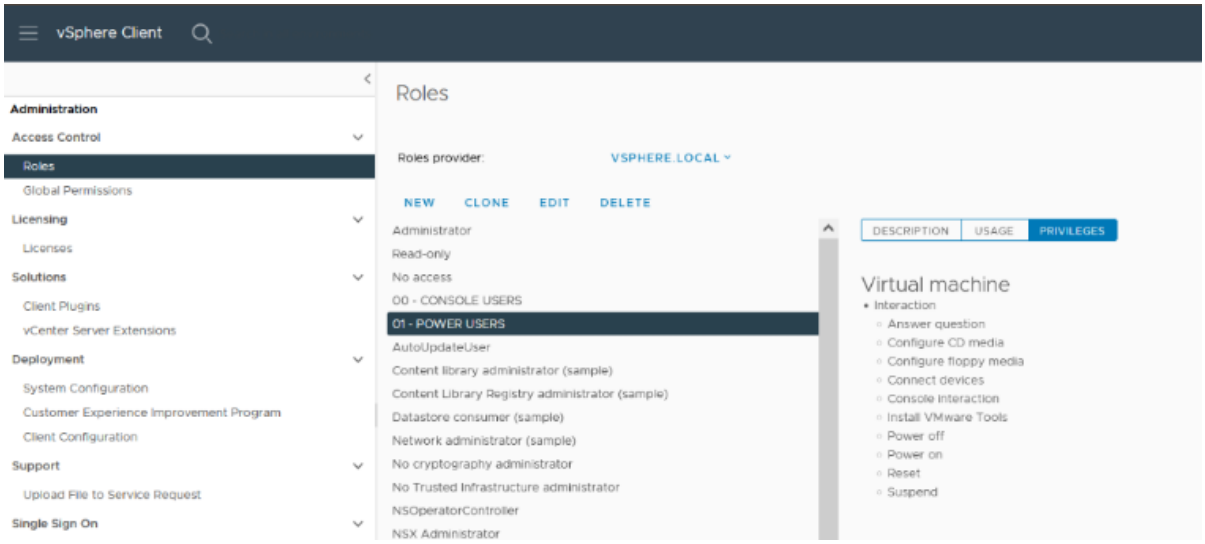


ROL: “00 - CONOLE USERS”

Interaction:

Answer question
Configure CD media
Configure floppy media
Connect devices
Console interaction
Install VMware Tools
Power off
Power on
Reset
Suspend

Tal com podem veure a la següent imatge:

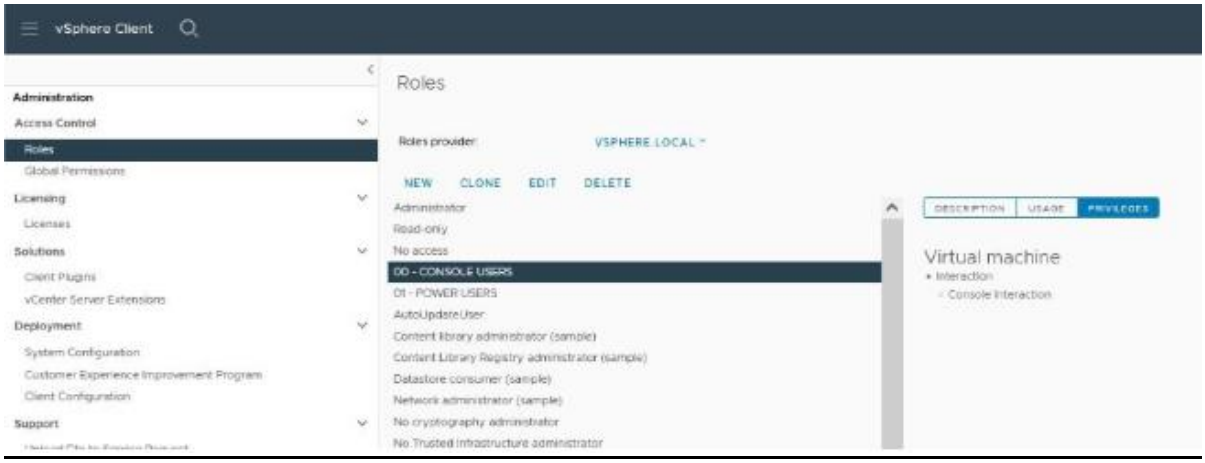


A la taula següent mostrem els grups del directori actiu i el ROL assignat.

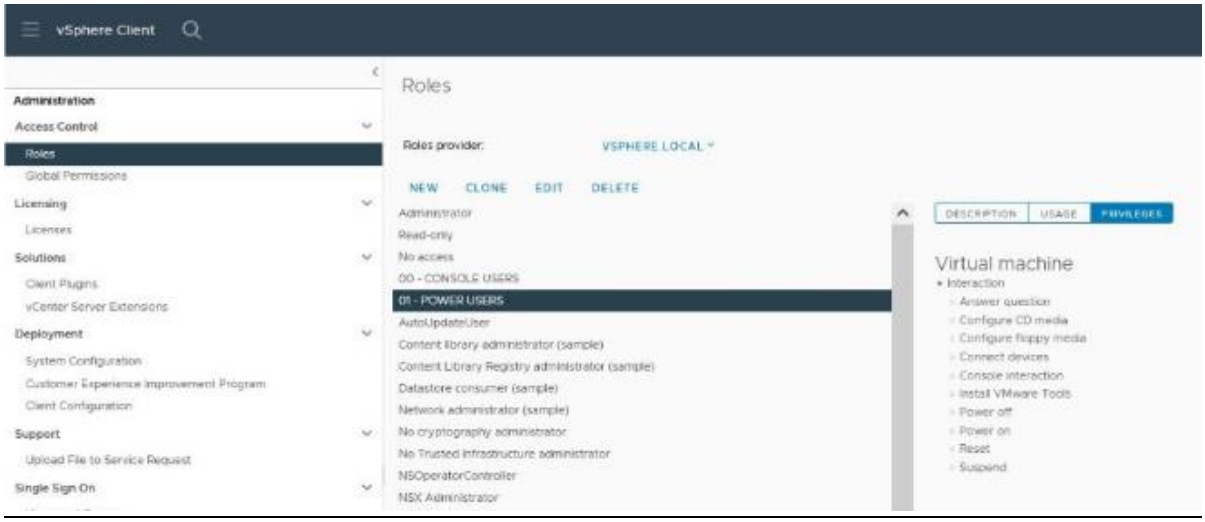
Grup de usuaris	ROL
ESEOG1OTGRVMA1	Té assignat el ROL “administrator” amb tots els privilegis.
ESEOG1OTGRVMA2	Té assignat el ROL “00 – CONSOLE USERS”.
ESEOG1OTGRVMA3	Té assignat el ROL “01 – POWER USERS”.

A la següent imatge veiem els privilegis definits per a cada grup d'usuaris que pertanyen al ROL “00 – CONSOLE USERS” i “01 – POWER USERS”.

<u>00 – CONSOLE USERS:</u>



01 – POWER USERS:



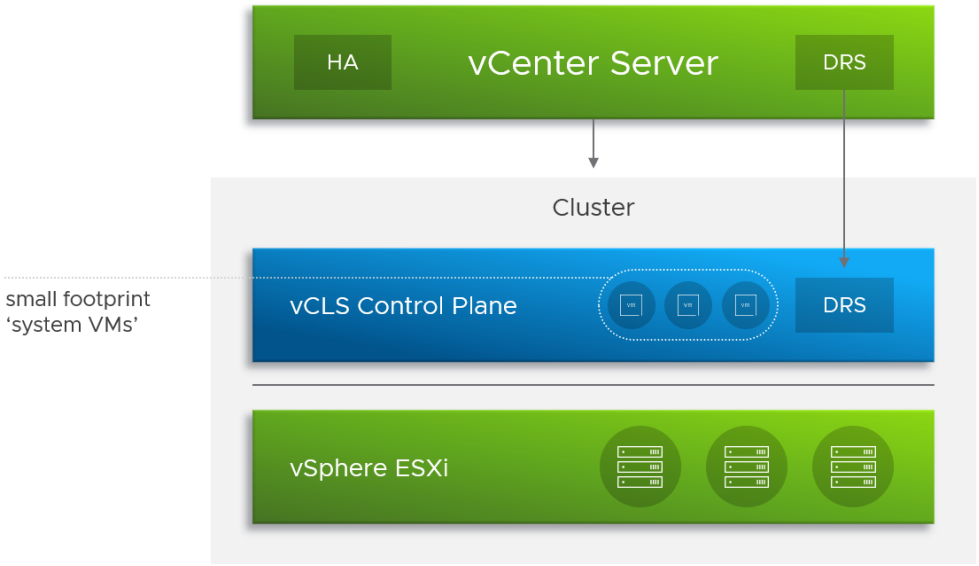
4.6.3 vSphere Cluster Services (vCLS)

vSphere Cluster Services és una característica de VMware vSphere que proporciona serveis de clusterització avançats per a clústers de servidors ESXi. Aquests serveis es fan servir per millorar la disponibilitat, la capacitat de recuperació i la gestió dels clústers en entorns de virtualització.

Alguns dels components i serveis clau de vSphere Cluster Services són:

- **High Availability (HA):** Proporciona una funcionalitat de protecció davant de falles en monitoritzar constantment l'estat dels hosts ESXi i les màquines virtuals. En cas d'error d'un host, les VM es reinicien automàticament en altres hosts disponibles.
- **Distributed Resource Scheduler (DRS):** Optimitza la utilització dels recursos de CPU i memòria en un clúster mitjançant la migració automàtica i equilibrada de màquines virtuals entre hosts en funció de la càrrega de treball.

- **Distributed Power Management (DPM):** Gestiona automàticament l'encesa i l'apagada de hosts dins del clúster segons la demanda de recursos, cosa que permet estalviar energia sense afectar la capacitat de resposta del clúster.
- **Proactive HA:** Detecta i respon de manera proactiva a esdeveniments i condicions que poden afectar la disponibilitat, com ara degradacions de maquinari o problemes de xarxa, prenent mesures preventives per minimitzar els impactes.



Vsphere Cluster Service (vCLS) s'habilita i executa per defecte a vSphere 7.0 i utilitza màquines virtuals com a agents per mantenir l'estat dels serveis del clúster per garantir que, si el servidor de vCenter deixa d'estar disponible, els serveis del clúster segueixen estant disponibles per mantenir els recursos i la integritat de les càrregues de treball que s'executen al clúster.

D'altra banda, els serveis de DRS i HA del clúster segueixen estan gestionats pel servidor vCenter i encara que aquests serveis no estiguin habilitats, vCenter crea automàticament les màquines virtuals vCLS gestionant la seva operativa i cicle de vida mitjançant serveis interns com ESX Agent Manager i Workload Control plane.

Depenent del nombre de host del clúster, es creen automàticament entre 1 i 3 màquines virtuals vCLS, sent 3 per a clústers de 3 o més host com és el nostre cas.

4.6.4 vRealize LogInsight

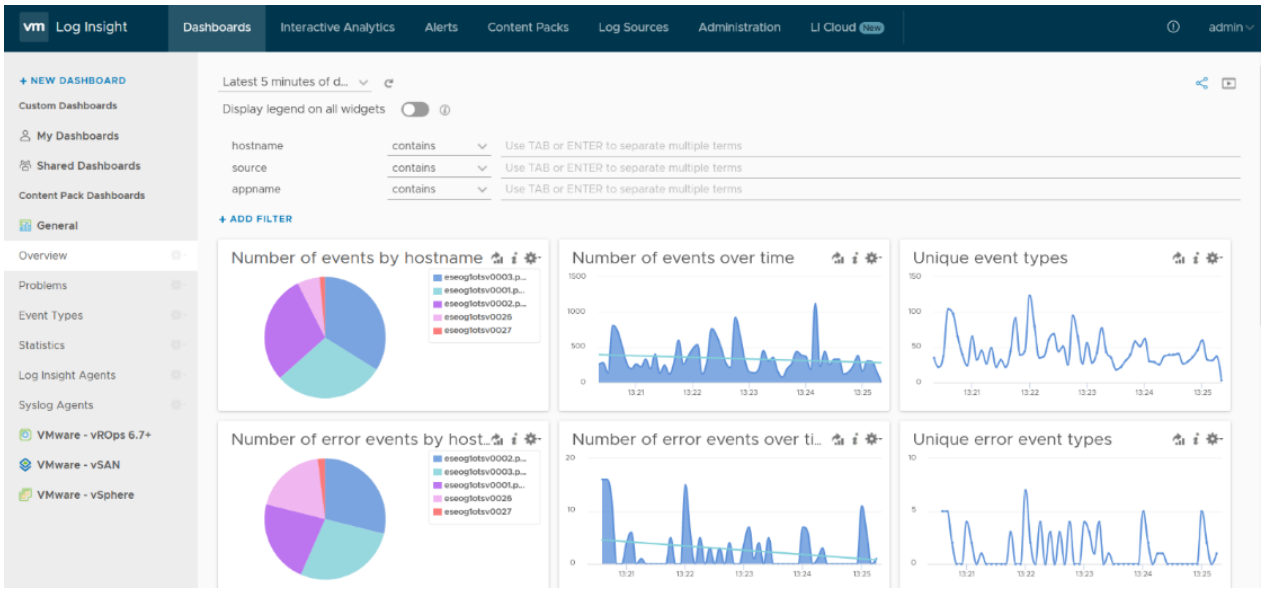
vRealize Log Insight és una solució d'administració i anàlisi de registres (logs) de VMware. Proporciona una plataforma centralitzada per recopilar, analitzar i visualitzar els registres generats per diversos components de la infraestructura, com ara servidors, aplicacions i dispositius de xarxa.

LogInsight proveeix monitorització en temps real de logs d'aplicació, traces de xarxa, fitxers de configuració, missatges i dades de rendiment així com ens ofereix una gestió de registres molt escalable, amb panells de gestió, anàlisis avançades i àmplia extensibilitat de tercers.

L'objectiu principal de vRealize Log Insight és ajudar els administradors de sistemes a comprendre i solucionar problemes al vostre entorn de manera eficient. Algunes de les funcionalitats clau de vRealize Log Insight són:

- Recopilació i agregació de registres: Permet recopilar registres de diferents fonts i consolidar-los en una ubicació centralitzada, cosa que en facilita la gestió i la recerca.
- Anàlisi i cerca ràpida: Utilitza potents capacitats de cerca i anàlisi en temps real per descobrir patrons, tendències i problemes potencials en els registres. Això ajuda a identificar i solucionar problemes de manera més ràpida i efectiva.
- Alertes i notificacions: Permet configurar alertes basades en esdeveniments específics en els registres, cosa que permet als administradors rebre notificacions immediates sobre problemes crítics o anomalies.
- Visualització i creació de panells: Ofereix una interfície intuïtiva i visual per mostrar i personalitzar panells de control i gràfics, cosa que facilita la visualització de dades i la generació d'informes.
- Integració amb altres eines de VMware: S'integra estretament amb altres solucions de VMware, com ara vSphere, vRealize Operations i vRealize Automation, cosa que permet una gestió i solució de problemes més holística.

Aquesta solució en proporciona una visibilitat de gran abast de les operacions i una solució ràpida de problemes en entorns físics i virtuals.



Configurem la VM amb els paràmetres següents:

Nom VMware vRealize LogInsight	Direcció IP
ESEOG1OTSV0028	10.14.162.62

A la taula següent es mostren els valors a la gestió:

Usuari Management	Accés
admin	https:// 10.14.162.62/login

5 SISTEMA DE BACKUPS OT ARCSERVE

5.1 INTRODUCCIÓ

El departament d'OT està immers en un ambiciós programa de transformació amb l'objectiu d'establir un sistema de backups sòlid i robust. La meta principal és garantir la capacitat de recuperació de dades de manera fiable, assegurant la immutabilitat de la informació.

La importància de comptar amb un sistema de còpies de seguretat fiable no pot subestimar-se. Les dades són l'actiu més valuós d'una organització i la pèrdua o la corrupció pot tenir conseqüències greus. Per això, el departament d'OT està enfocat a implementar una estratègia que asseguri la protecció de les dades crítiques.

Aquest programa de transformació implica l'avaluació i la millora dels processos existents, així com l'adopció de tecnologies avançades. S'estan implementant solucions de backup i recuperació d'última generació, que permetran fer còpies de seguretat de forma periòdica i automàtica. A més, s'està treballant en la creació de polítiques i procediments clars per garantir la integritat de les dades i la seva disponibilitat en cas de fallades.

L'objectiu final és establir un sistema de còpies de seguretat sòlid i robust que garanteixi la confiança i la immutabilitat de les dades. Això proporcionarà tranquil·litat a l'organització i assegurarà que, en cas d'un incident, les dades es puguin recuperar de manera ràpida i eficient, minimitzant així l'impacte operatiu i protegint la continuïtat del negoci.

5.2 SOLUCIÓ PROPOSADA

La solució proposada serà la integració d'un appliance Arcserve UDP per a copies de seguretat amb una cabina immutable Onexafe per a emmagatzemar les repliques dels backups.

Arcserve UDP

Arcserve UDP (Unified Data Protection) és una solució integral de protecció de dades que ofereix una àmplia gamma de capacitats per recolzar i recuperar informació crítica de manera eficient i fiable.

Arcserve UDP combina la còpia de seguretat basada en imatges, la replicació, la deduplicació global i la recuperació davant de desastres en una única plataforma unificada. Aquesta solució permet a les organitzacions protegir les dades en entorns físics, virtuals i al núvol, assegurant la continuïtat del negoci i minimitzant el risc de pèrdua d'informació.

La característica clau d'Arcserve UDP és el vostre enfocament en la simplicitat i la facilitat d'ús. Amb una interfície intuïtiva, els administradors poden configurar polítiques de còpia de seguretat personalitzades i automatitzades, definir finestres de temps i recuperació i monitoritzar l'estat de les còpies de seguretat de manera centralitzada.

A més, Arcserve UDP ofereix capacitats avançades de recuperació granular, permetent la restauració d'arxius individuals, aplicacions completes o fins i tot sistemes sencers en

minuts. Això garanteix la disponibilitat i la continuïtat del negoci davant de qualsevol incident o desastre.

Arcserve UDP també proporciona una eficient deduplicació global, que redueix significativament l'espai d'emmagatzematge necessari i optimitza els recursos de xarxa per a una transferència més ràpida de dades.

Cabina immutable OneXafe

Les cabines immutables OneXafe són solucions d'emmagatzematge dissenyades per proporcionar una protecció robusta i fiable de les dades. La característica principal d'aquestes cabines és la seva capacitat per mantenir la immutabilitat de les dades emmagatzemades, cosa que significa que les dades no poden ser alterades ni esborrades de manera accidental o maliciosa.

OneXafe utilitza tecnologia de snapshots (instantànies) i l'aplicació de polítiques de retenció per garantir la immutabilitat de les dades. Els snapshots capturen una imatge instantània de l'estat de les dades en un moment específic i aquestes instantànies es mantenen inalterables segons les polítiques establertes. Això proporciona una protecció addicional contra la manipulació, el ransomware o altres intents de corrupció o eliminació de dades.

Aquestes cabines immutables són altament escalables i ofereixen un rendiment eficient per a la gestió i protecció de grans volums de dades. A més, la seva arquitectura distribuïda i resistent a fallades assegura la disponibilitat contínua de les dades fins i tot en cas de falla de components.

La immutabilitat de les dades a les cabines OneXafe és especialment valuosa en entorns on es requereix complir regulacions i normatives de seguretat de dades, com es en el nostre cas per la protecció d'informació.

5.3 GENERALITATS DEL ENTORN

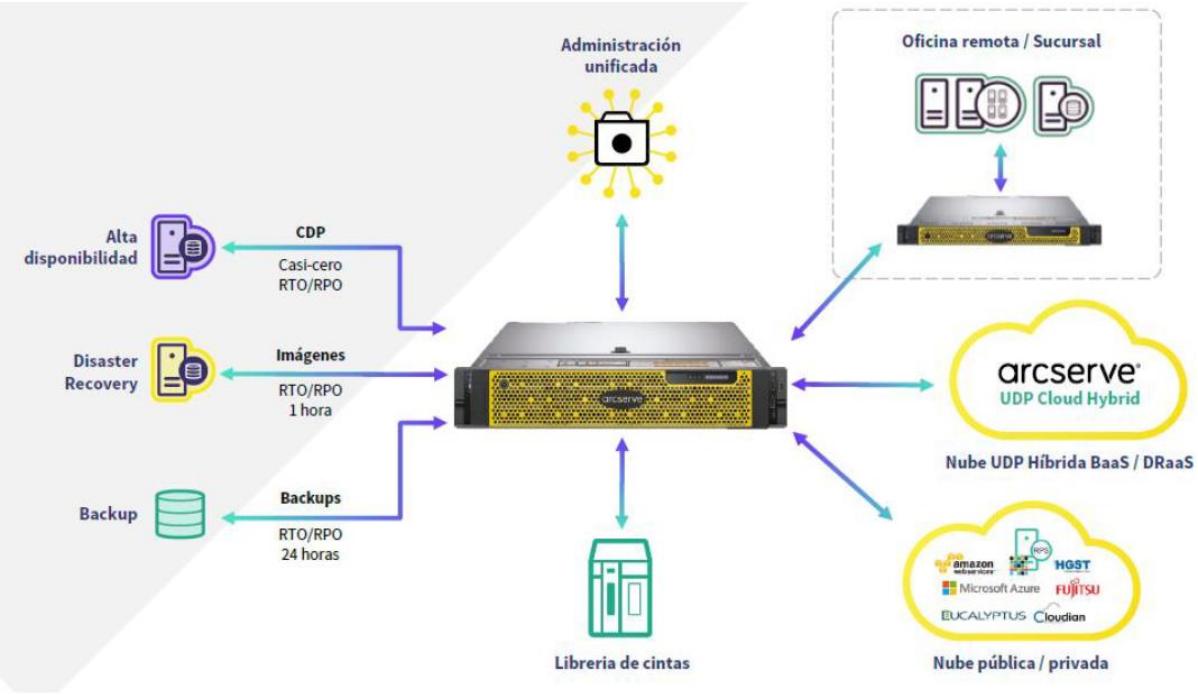
5.3.1 Appliance Arcserve

Arcserve proporciona solucions per protegir els actius digitals d'organitzacions que necessiten protecció de dades integral i a una escala total. Arcserve proporciona solucions de continuïtat empresarial que protegeixen infraestructures amb aplicacions i sistemes a qualsevol lloc.

• Protecció en una única seu per a sistemes físics i virtuals, incloent x86 i no x86.

• Replicació dels backups a una cabina immutable.

• Desplegament híbrid amb una combinació de sistemes físics i virtuals.



L'appliance proposat per a la nostra solució serà el model 9048 d'Arcserve.

En la següent taula es mostren les seves principals característiques:

CPU	RAM	Capacitat Utilitzable	Capacitat Efectiva
Intel Xeon Silver 4108 1,8 GB	48 GB	16 TB	48 TB

Addicionalment compta amb les següents característiques:

- Kits d'Expansió per augmentar la capacitat i respondre a la demanda del creixement de les dades.
- Compte amb 2 fonts d'alimentació redundades.
- Disaster recovery (InstantVM) per executar una màquina virtual al mateix appliance a partir d'un punt de restauració
- Replicació de Jobs a unitats d'arxivat externes
- Assistència de maquinari in situ en 4 hores
- Garantia de la seguretat de dades i sistemes tant en línia com emmagatzemats amb xifratge integrat AES/SSL i TLS 1.2.

5.3.2 Cabina Immutable OneXafe

Per a l'arxivat a una segona unitat d'emmagatzematge, s'ha instal·lat una cabina amb 96TB d'emmagatzematge brut immutable. Aquesta cabina pot estar al mateix site que l'appliance o al site remot per fer còpies creuades.

L'emmagatzematge d'OneXafe protegeix les dades amb snapshots continues i immutables cada 90 segons. Una snapshot immutable és una còpia de les dades que ni el ransomware, els usuaris ni el programari de backups poden sobreescriure o eliminar.

Totes les dades que s'emmagatzemen a la cabina d'arxivat es poden recuperar fàcilment en cas que pateixin danys, s'eliminin, hi hagi atacs de ransomware o altres errors. No cal restaurar la informació des de la darrera còpia de seguretat, només cal buscar-la i restaurar-la.

OneXafe realitza una deduplicació en línia a les snapshots contínues, la qual cosa redueix la petjada de dades alhora que garanteix la recuperació de la informació independentment de la seva mida (de TB a PB), en menys de 15 segons.

A la taula següent es mostren les principals característiques de la cabina:

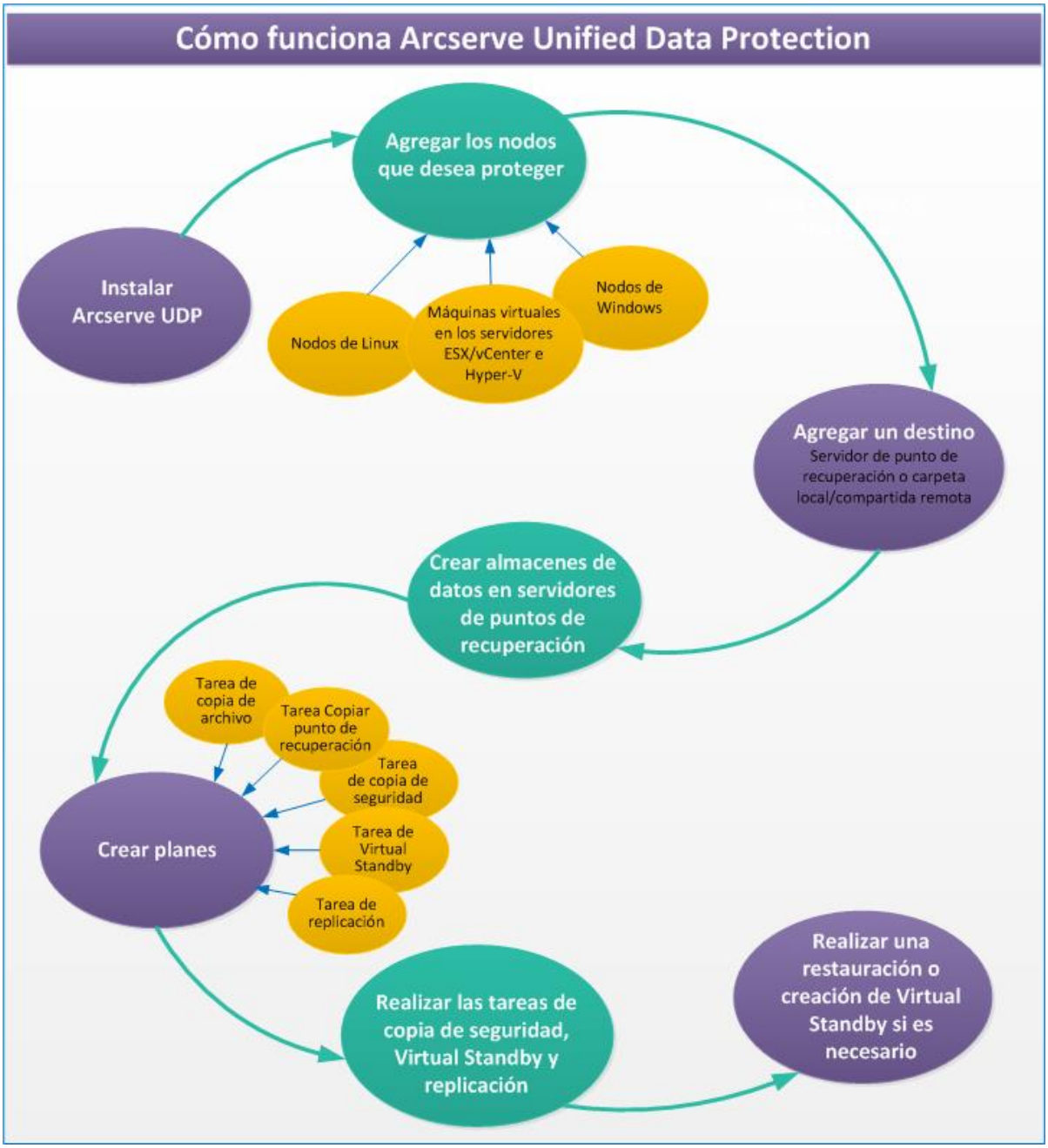
Requisits d'entrada	100-240 V CA, 10,7–4,2 A máx.
Alimentació	Sortida d'alimentació doble 750 W; voltajes de sortida +12 V (75 A), +5 Vsb (4 A)
Pes (en buit, sense discos)	33,1 kg (73 lb)
Requisits d'espai (amplada × profunditat × altura)	434 × 42,8 × 75,55 mm (19 × 3,4 × 28,1 pulgadas); 2 unitats en bastidor
Tipus de disc dur	SATA de 3,5 pulgades (6 Gb/s)/SAS (6 Gb/s y 12 Gb/s)
Temperatura i humitat en funcionament	De 10 °C a 35 °C (de 50 °F a 95 °F)
Refrigeració	6 ventiladors de velocitat variable
Protocols de servei d'arxius	SMB (1.0, 2.0, 2.1, 3.0); NFS v3
Ports Gigabit Ethernet	4 × 10 GbE BASE-T o bien 4 × 10 GbE SFP+
Ports USB	2 × USB 3.0 (frontal)
Administració d'accés remot	iDRAC a través de port 1 GbE
Emissions electromagnètiques i compatibilitat	FCC Classe A, EN 55022 Classe A, EN 61000-3-2/-3- 3, CISPR 22 Classe A
Bahías de unitats de discos	Fins 12 × 3,5 pulgades (frontal)
Capacitat bruta màxima	144 TB (12 discos de 12 TB cada un)

5.3.3 Arcserve UDP

Arcserve UDP és una solució de protecció de dades unificada que permet protegir sistemes informàtics. Arcserve UDP utilitza els següents passos de nivell alt per protegir els sistemes.

1. Instal·lació d'Arcserve UDP.
2. Afegir els equips que es volen protegir:
    - Es poden afegir màquines virtuals i equips de Windows o Linux a servidors ESXi/vCenter, servidors Hyper-V i servidors Nutanix AHV.
3. Afegir una destinació:
    - Una destinació pot ser un servidor de punt de recuperació, carpeta local o carpeta compartida remota.
4. Crear magatzems de dades a servidors de punts de recuperació:
    - Un magatzem de dades és una zona física dun disc. Es poden crear magatzems de dades de deduplicació i de no deduplicació.
5. Crear un pla:
    - Un pla és un grup de tasques per gestionar la còpia de seguretat, la replicació, la còpia de punt de recuperació, la còpia en cinta, la creació de màquines de Virtual Standby o la prova de recuperació assegurada. També podeu afegir Ruta UNC, node de l'Office 365 Exchange Online, node SharePoint Online o node OneDrive i crear tasques relacionades.
6. Realitzar tasques com a còpia de seguretat, crear Virtual Standby i replicació.
7. Realitzar una restauració simple o una reconstrucció completa.

El diagrama següent il·lustra els passos de nivell alt que cal fer per protegir dades:



Instal·lem la següent versió d'ArcServe UDP a la infraestructura del projecte:

Versió ArcServe UDP	8.1 build 8.0.5628.430

5.3.4 Deduplicació Arcserve

La deduplicació a Arcserve Unified Data Protection (UDP) és una funció clau que permet reduir l'emmagatzematge necessari per donar suport a les dades, optimitzant l'ús de

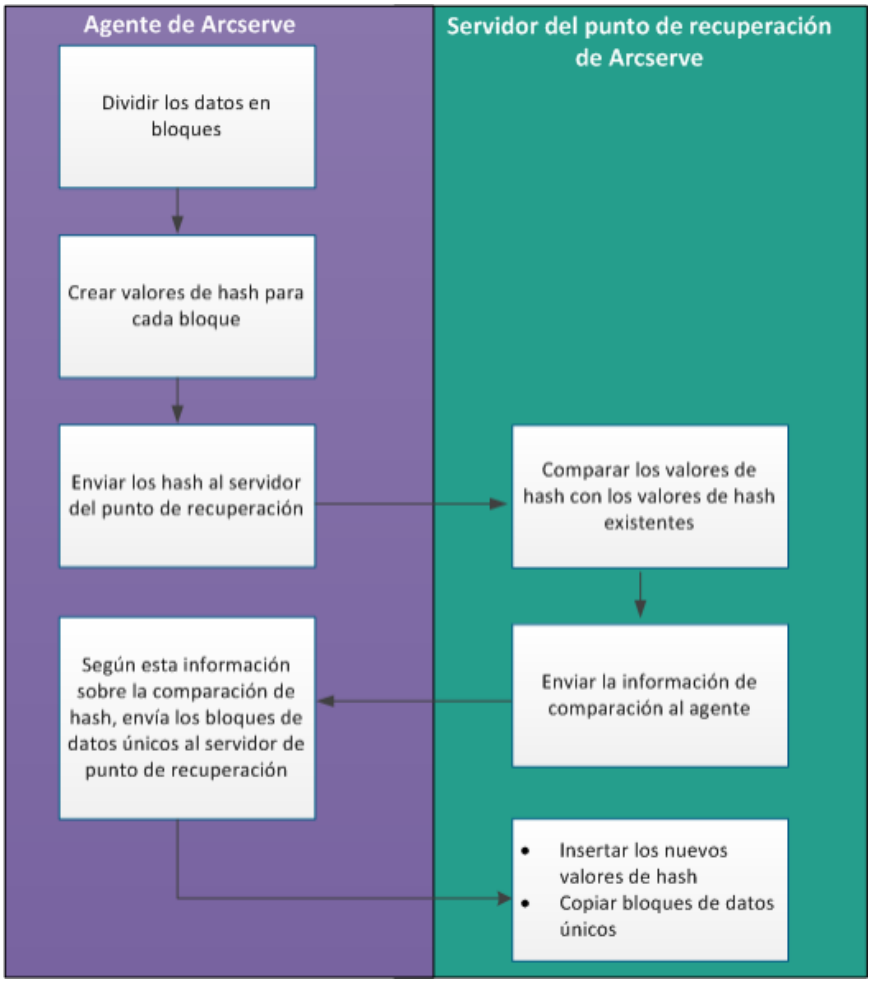
recursos i millorant l'eficiència en la transferència d'informació. Utilitza una tècnica de deduplicació global, que s'aplica a múltiples nivells: dins de cada màquina virtual, entre diferents màquines virtuals i a nivell global a tot l'entorn de seguretat.

La deduplicació global elimina la redundància de dades en identificar i emmagatzemar només les parts úniques dels fitxers. Això s'aconsegueix mitjançant algoritmes sofisticats que analitzen les dades i creen segments d'informació que es poden compartir i referenciar entre diferents còpies de seguretat. Això redueix considerablement l'espai requerit per emmagatzemar les dades, la qual cosa al seu torn redueix els costos d'emmagatzematge i millora l'eficiència en la transferència de dades a través de la xarxa.

A més, la deduplicació a Arcserve UDP és altament eficient i es realitza en temps real, cosa que significa que les dades es dedupliquen en el moment de la còpia de seguretat sense afectar el rendiment del sistema.

El procés de deduplicació d'Arcserve UDP divideix les dades en blocs de dades ia cada bloc se li assigna un identificador únic anomenat hash. Hash es calcula basant-se en el clúster de volums. La mida del bloc de deduplicació per defecte és de 4 kB (la mida del clúster de volums predeterminat és de 4 kB per a la majoria dels nodes). Aquests valors de hash es comparen amb els valors de hash de les dades de còpia de seguretat existents i si hi ha referències duplicades, no es realitzarà la còpia de seguretat d'aquests blocs de dades. Només es fa la còpia de seguretat dels blocs de dades amb referències úniques.

El diagrama següent mostra com funciona la deduplicació a Arcserve UDP:



Quan s'activa una còpia de seguretat, el procés de deduplicació a l'agent primer divideix les dades en blocs i assigna una clau de hash o valor únics a cada bloc. Els paràmetres de hash s'envien a continuació al servidor de punt de recuperació. Al servidor de punt de recuperació, aquests valors de hash es comparen amb els valors de hash existents i es filtren els hashs duplicats. Els resultats de la comparació es retornen a l'agent. Segons aquesta informació de hash duplicada, l'agent envia els blocs de dades únics al servidor de punt de recuperació per fer la còpia de seguretat. Els valors de hash nous d'aquests blocs de dades també s'insereixen a la llista de hash existents al servidor de punt de recuperació.

A continuació, es mostren els beneficis d'utilitzar la deduplicació de dades a Arcserve UDP:

- Còpia de seguretat completa més ràpida
- Tasca de combinació més ràpida
- Compatibilitat amb la deduplicació global
- Replicació optimitzada

Dins de les configuracions dels dos “Recovery Point Server”, s'ha assignat una deduplicació alta (4 KB de mida de bloc) per al datastore Data_Store1, que s'encarregarà d'emmagatzemar les còpies de seguretat principals, i s'ha assignat una deduplicació baixa (32 KB de mida de bloc) per al datastore Data_Store2, que s'encarregarà d'emmagatzemar les rèpliques de les còpies de seguretat principals.

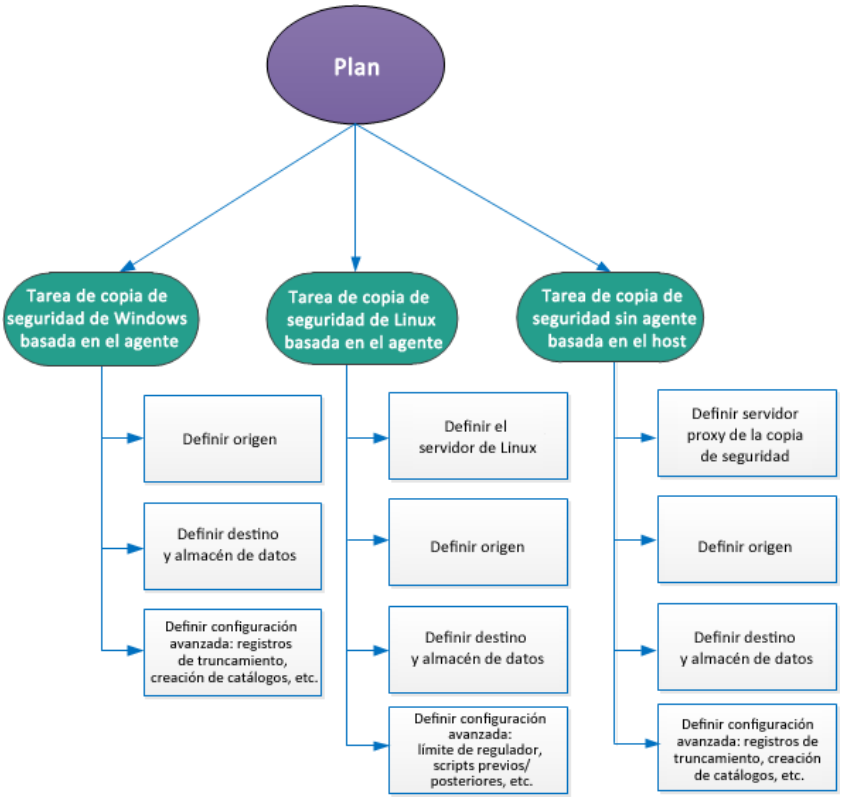
5.3.5 Funcionament dels plans a Arcserve

Per protegir un node, cal crear un pla amb una tasca de còpia de seguretat. Un pla és un grup de tasques per gestionar la còpia de seguretat, la replicació i la creació de nodes de Virtual Standby. Un pla està format per una única tasca o per diverses. Les tasques són un conjunt d'activitats per definir l'origen, la destinació, la programació i els paràmetres avançats.

Es poden crear les tasques següents:

- **Còpia de seguretat de Windows basada en l'agent:** Definim una tasca de còpia de seguretat per protegir equips amb sistema operatiu Windows. Realitzem la instal·lació de l'agent d'ArcServe l'equip per fer-hi la còpia del sistema.
- **Còpia de seguretat sense agent basada al host:** Definim una tasca de còpia de seguretat per protegir màquines virtuals basades en un servidor de vCenter o ESXi de VMware.
  En un mètode de còpia de seguretat no utilitzeu agent, per la qual cosa no cal instal·lar cap component al servidor o a la màquina virtual. No obstant això, haurem d'instal·lar l'agent en un servidor intermediari per poder fer les còpies de seguretat.
- **Linux, basada en l'agent:** Definim una tasca de còpia de seguretat per protegir equips basats en Linux. Realitzem la instal·lació de l'agent al servidor de backups i no als equips que es vol protegir.

El diagrama següent mostra un pla amb diferents tasques de còpia de seguretat i els paràmetres de cadascuna.



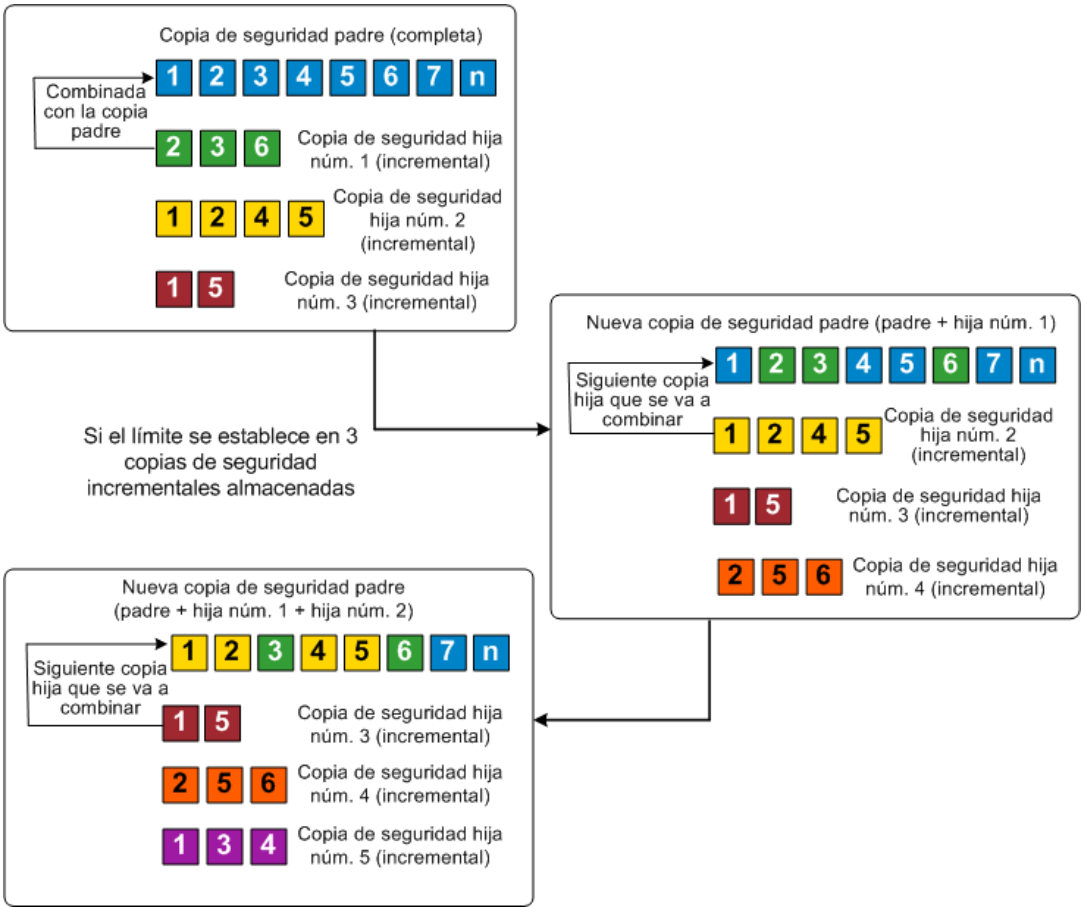
5.3.6 Mètodes de backup

Arcserve UDP a diferencia de altres solucions de backup tradicionals utilitza per ser més òptim un el mètode de còpies de seguretat d'incrementals infinites.

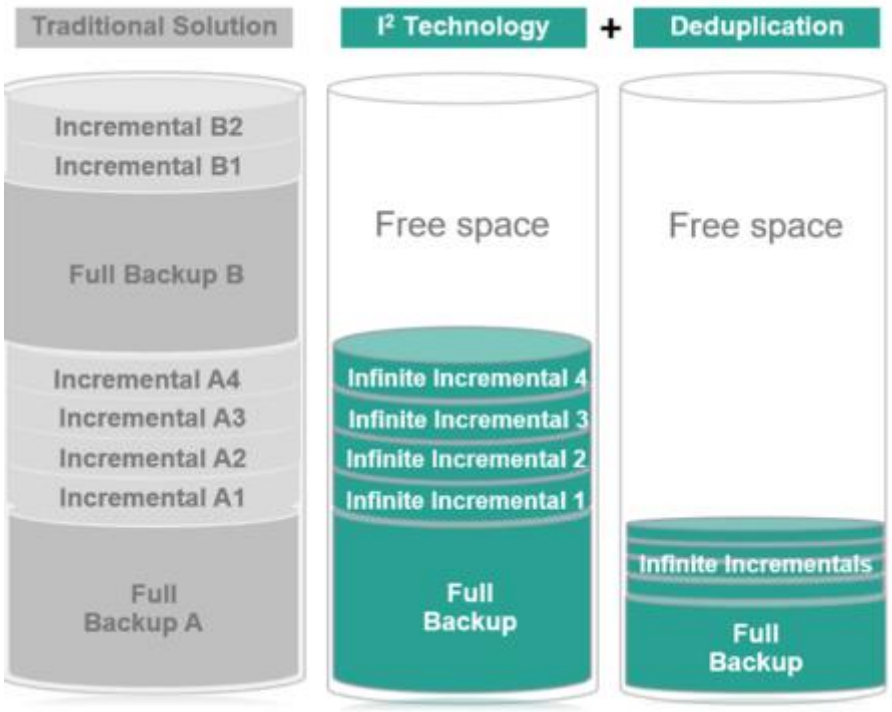
Les instantànies periòdiques acumularan una cadena gran de blocs amb còpia de seguretat que s'ha de controlar cada vegada que es faci una còpia de seguretat nova, i requereixen també un espai addicional per emmagatzemar les imatges de còpia de seguretat en creixement continu. Per minimitzar aquest problema potencial, l'Agent d'Arcserve UDP (Windows) utilitza el procés de còpia de seguretat incremental il·limitada, que crea de manera intel·ligent còpies de seguretat d'instantània incrementals per sempre (després de la còpia de seguretat completa inicial) i utilitza menys espai d'emmagatzematge, realitza còpies de seguretat més ràpides i posa menor càrrega en els servidors de producció.

Les còpies de seguretat incrementals infinites us permeten establir un límit per al nombre de còpies de seguretat secundàries incrementals que s'han d'emmagatzemar.

En superar el límit especificat, Arcserve combinarà la còpia de seguretat secundària incremental més antiga amb la còpia de seguretat principal per crear una nova imatge de línia de referència que està formada pels blocs "principal més secundari més antic" (els blocs no modificats es quedaran igual). El cicle de la combinació de la còpia de seguretat secundària més antiga amb la còpia de seguretat principal es repetirà per a totes les còpies de seguretat posteriors, permetent fer còpies de seguretat d'instantànies incrementals il·limitades, mentre es manté el mateix nombre d'imatges de còpia de seguretat (i de control) emmagatzemat.



D'aquesta manera i sumant-li la deduplicació que s'aplica a cada tasca, obtindrem una reducció considerable en emmagatzematge, a diferència del que ocuparia en una solució tradicional.



5.4 PLANS COPIES DE SEGURETAT

5.4.1 Replicació backups Arcserve

Per tal de donar més seguretat sobre les dades, hem configurat una tasca de replicació que es realitzarà cada vegada que s'executi una còpia de seguretat, aquesta tasca de replicació es defineix dins de cada pla configurat.

A la solució implementada els backups es replicaran al datastore de la cabina immutable situada a al CPD 2 (Data_Store2), amb una retenció definida segons criticitat que s'explica en els apartats següents.

5.4.2 Configuració plans

Per garantir la recuperació dels sistemes (OT) i la informació d'automatització de la planta de Esplugues, en base a la criticitat d'aquests, s'han creat 3 plans de còpies de seguretat.

- Pla Nivell 1 Criticitat
- Pla Nivell 2 Criticitat
- Pla Nivell 3 Criticitat

La còpia de seguretat que realitzen els 3 plans s'emmagatzema localment al Datastore “Data_Store1”.

Addicionalment a cada pla es configura una tasca de replicació de les còpies de seguretat a la cabina immutable ubicada al CPD 2.

5.4.2.1 Pla nivell 1 de criticitat

Aquest pla es el nivell mes baix de criticitat, està configurat per als equips i sistemes que requereixen una còpia de seguretat mensual.

Pla	Periodicitat	Data	Hora	Tipus
Pla Nivell 1	Mensual	Últim Diumenge del mes	3:00 AM	Incremental

Dins aquest pla s'han configurat les tasques següents:

Tasca	Descripció	Destí	Ubicació
Task 1	Backup: Host-Base Agentless	Data_Store1	CPD 2
Task 2	Replicate	Data_Store2	CPD 1

Al pla de nivell 1 s'ha configurat la retenció de les còpies de seguretat local i la replicació a la cabina immutable amb els paràmetres següents:

Pla	Tasca	Periodicitat	Emmagatzematge	Ubicació	Retenció
Pla Nivell 1	Task 1	Mensual	Data_Store1	CPD 1	12 meses
Pla Nivell 1	Task 2	Mensual	Data_Store2	CPD 2	120 meses

5.4.2.2 Pla nivell 2 de criticitat

Aquest pla es el nivell intermedi de criticitat, està configurat per als equips i sistemes que requereixen una còpia de seguretat mensual i una setmanal.

Pla	Periodicitat	Data	Hora	Tipus
Pla Nivell 2	Mensual	Ultimo Diumenge del mes	1:00 AM	Incremental
Pla Nivell 2	Setmanal	Cada Diumenge	1:00 AM	Incremental

Dins aquest pla s'han configurat les tasques següents:

Tasca	Descripció	Destí	Ubicació
Task 1	Backup: Host-Base Agentless	Data_Store1	CPD 1
Task 2	Replicate	Data_Store2	CPD 2

Al pla de nivell 2 s'ha configurat la retenció de les còpies de seguretat local i la replicació a la cabina immutable amb els paràmetres següents:

Pla	Tasca	Periodicitat	Emmagatzematge	Ubicació	Retenció
Pla Nivell 2	Task 1	Setmanal	Data_Store1	CPD 1	5 setmanes
Pla Nivell 2	Task 2	Setmanal	Data_Store2	CPD 2	5 setmanes
Pla Nivell 2	Task 1	Mensual	Data_Store1	CPD 1	12 mesos
Pla Nivell 2	Task 2	Mensual	Data_Store2	CPD 2	120 mesos

5.4.2.3 Pla nivel 3 de criticitat

Aquesta pla es el nivell mes alt de criticitat per tant, està configurat per als equips i sistemes que requereixen una còpia de seguretat mensual, una setmanal i una diària.

Pla	Periodicitat	Data	Hora	Tipus
Pla Nivell 3	Diària	L-M-X-J-V-S	3:00 AM	Incremental
Pla Nivell 3	Setmanal	Cada Diumenge	3:00 AM	Incremental
Pla Nivell 3	Mensual	Ultimo Diumenge del mes	3:00 AM	Incremental

Dins aquest pla s'han configurat les tasques següents:

Tasca	Descripció	Destí	Ubicació
Task 1	Backup: Host-Base Agentless	Data_Store1	CPD 1
Task 2	Replicate	Data_Store2	CPD 2

Al pla de nivell 2 s'ha configurat la retenció de les còpies de seguretat local i la replicació a la cabina immutable amb els paràmetres següents:

Pla	Tasca	Periodicitat	Emmagatzematge	Ubicació	Retenció
Pla Nivell 3	Task 1	Diària	Data_Store1	CPD 1	7 dies
Pla Nivell 3	Task 2	Diària	Data_Store2	CPD 2	7 dies
Pla Nivell 3	Task 1	Setmanal	Data_Store1	CPD 1	5 setmanes
Pla Nivell 3	Task 2	Setmanal	Data_Store2	CPD 2	5 setmanes
Pla Nivell 3	Task 1	Mensual	Data_Store1	CPD 1	12 mesos
Pla Nivell 3	Task 2	Mensual	Data_Store2	CPD 2	120 mesos

6 GLOSSARI

Cisco Systems: Un proveïdor líder en tecnologies de xarxes i comunicacions, que ofereix una àmplia gamma de productes i solucions per a empreses i organitzacions.

Dell EMC: Un fabricant de solucions tecnològiques que ofereix infraestructures de TI, inclosos servidors, emmagatzematge, xarxes i altres components.

VMware: Una empresa especialitzada en virtualització de servidors i infraestructures de núvol, que ofereix solucions com el VMware vSphere i el VMware vSAN.

Hewlett Packard Enterprise (HPE): Una empresa líder en tecnologia que ofereix una àmplia gamma de productes, incloent servidors, emmagatzematge, xarxes i solucions de gestió de centres de dades.

Nutanix: Un fabricant de solucions d'infraestructura hiperconvergent que combina servidors, emmagatzematge i xarxes en una única plataforma integrada.

Lenovo: Un fabricant de tecnologia que ofereix servidors, emmagatzematge i altres solucions per a centres de dades i empreses.

NetApp: Un proveïdor de solucions d'emmagatzematge empresarial, incloent-hi sistemes de fitxers, emmagatzematge en núvol i altres serveis relacionats.

Red Hat: Una empresa especialitzada en solucions de programari de codi obert, incloent-hi la plataforma de virtualització Red Hat Virtualization.

Entorn industrial: Un entorn que inclou infraestructures, sistemes i equips utilitzats en processos de producció i control industrial.

Paradigma de seguretat: Un enfocament o conjunt de principis que guien les pràctiques de seguretat en un sistema o entorn determinat.

Estàndards: Normes o criteris establerts per a garantir la coherència, interoperabilitat i seguretat en un determinat àmbit o indústria.

IEC/ISA62443: Norma de ciberseguretat industrial desenvolupada per la International Electrotechnical Commission (IEC) i l'International Society of Automation (ISA).

NIST 800-82: Estàndard del National Institute of Standards and Technology (NIST) dels Estats Units per a la ciberseguretat de sistemes industrials.

Segmentació de xarxa: Divisió de la xarxa en segments més petits per aïllar i protegir diferents parts o components del sistema.

ISA99/IEC62443: Estàndard de segmentació de xarxa per a la ciberseguretat industrial desenvolupat per la International Society of Automation (ISA) i l'International Electrotechnical Commission (IEC).

Comitè de la Societat Internacional d'Automatització (ISA): Un organisme que desenvolupa i promou estàndards per a la indústria d'automatització i control.

Comissió Electrotècnica Internacional (IEC): Un organisme que desenvolupa i publica normes internacionals en el camp de l'electrotècnica.

Capes de comunicació: Nivells jeràrquics en què es divideixen les funcions i les comunicacions d'un sistema de xarxa.

DMZ (Zona Desmilitaritzada): Una subxarxa aïllada que s'utilitza per a allotjar serveis o dispositius exposats a xarxes externes i proporcionar una capa addicional de seguretat.

Xarxa IT: La part de la xarxa que es dedica als sistemes i serveis d'informàtica tradicionals.

Xarxa OT: La part de la xarxa que es dedica als sistemes i serveis d'automatització i control industrial.

Infraestructura hiperconvergent (HCI): Un sistema unificat definit per programari que combina emmagatzematge, recursos de còmput, xarxa i gestió en una única plataforma.

Cabines de discos: Dispositius de emmagatzematge físic que contenen discos durs per a l'emmagatzematge de dades.

Escalabilitat: Capacitat d'un sistema per adaptar-se i gestionar un augment de càrrega o demanda de manera eficient.

Entorns crítics: Infraestructures o sistemes que són essencials per al funcionament d'una organització o procés.

Appliance: Un dispositiu o sistema completament integrat i preconfigurat per realitzar una tasca específica.

Consola: Una interfície gràfica o de línia de comandes que permet controlar i gestionar un sistema informàtic o una aplicació.

Virtualització: Tecnologia que permet crear i gestionar màquines virtuals, és a dir, entorns virtuals que funcionen independentment del maquinari físic.

Clúster: Un grup de nodes o servidors que treballen conjuntament per a realitzar una tasca o proporcionar un servei.

Obsolescència: Estat en què un dispositiu o tecnologia esdevé desactualitzat o ineficient a mesura que es desenvolupen nous avenços o alternatives.

OT (Operational Technology): Tecnologia utilitzada per gestionar i controlar processos físics, com ara la producció o les operacions industrials.

DR (Disaster Recovery): Procés de restauració de les operacions i els serveis després d'un desastre o una interrupció significativa.

Escalat transparent: Capacitat d'un sistema per adaptar-se i augmentar la seva capacitat de manera invisible per als usuaris o les aplicacions.

Best practices: Pràctiques o mètodes recomanats que s'han demostrat com a eficients i efectius en un determinat context.

Escalabilitat vertical: Increment de la capacitat d'un sistema augmentant els recursos d'un únic node o servidor.

Escalabilitat horitzontal: Increment de la capacitat d'un sistema afegint més nodes o servidors al clúster existent.

Immutabilitat de la informació: L'immutabilitat de la informació fa referència a la seva característica de ser inalterable o no modificable. En el context de les còpies de seguretat, garantir la immutabilitat de les dades significa assegurar que no es puguin alterar, esborrar o corrompre accidentalment o de manera maliciosa.