**CỤC THUẾ**

**------\*\*\*------**

|  |
| --- |
| C:\Users\chung\Desktop\Thue.png |

**TÀI LIỆU THIẾT KẾ BỔ SUNG**

**MÁY CHỦ DATABASE HDDT TẠI DRC**

**Hợp đồng 36/2024/HĐKT/TCT-FPT IS-FTI**

**Gói thầu: “Dịch vụ chuyển thiết bị tới địa điểm thuê**

**trung tâm dữ liệu”**

**Chủ đầu tư:**

**Cục Thuế**

**Đơn vị thi công:**

**Công ty TNHH FPT IS**

**Hà Nội, 2025**

Hà Nội, ngày…tháng….năm 2010

**Mục lục**

[I.1. Thiết kế hệ thống máy chủ CSDL HDDT bổ sung tại TTDL dự phòng 2](#_Toc193978825)

[I.1.1. Mô hình triển khai Cơ sở dữ liệu 2](#_Toc193978826)

[I.1.2. Thiết kế chi tiết hệ thống máy chủ Docs 5](#_Toc193978827)

[I.1.3. Thiết kế chi tiết hệ thống máy chủ Ana 35](#_Toc193978828)

[I.2. Thiết kế hệ thống máy chủ CSDL MTT bổ sung tại TTDL dự phòng 85](#_Toc193978829)

[I.2.1. Mô hình triển khai Cơ sở dữ liệu 85](#_Toc193978830)

[I.2.1. Thiết kế chi tiết hệ thống máy chủ Search 89](#_Toc193978831)

[I.2.2. Thiết kế chi tiết hệ thống máy chủ Transaction 117](#_Toc193978832)

[I.2.3. Thiết kế chi tiết hệ thống máy chủ Docs 145](#_Toc193978833)

[I.2.4. Thiết kế chi tiết hệ thống máy chủ Ana 174](#_Toc193978834)

## Thiết kế hệ thống máy chủ CSDL HDDT bổ sung tại TTDL dự phòng

### Mô hình triển khai Cơ sở dữ liệu

Tại trung tâm dữ liệu dự phòng, các máy chủ cơ sở dữ liệu được cài đặt và cấu hình thành 01 Cluster Database: Cluster HDDT

Các cluster này cũng được quản trị, giám sát bằng các máy chủ quản trị OpsCenter chạy HA, quản trị chung cả hệ thống CSLD tại trung tâm dữ liệu chính và dự phòng. Trên các cluster tạo ra các DC phục vụ các workload khác nhau bao gồm: DR\_Trans, DR\_Search, DR\_Docs và DR\_Ana.

Hệ thống máy chủ CSDL của ứng dụng hóa đơn điện tử được bổ sung tạm (phục vụ chuyển đổi DC sang DC mới) lấy máy từ hợp đồng số 34/2024/HĐKT/TCT-TECAPRO-OSP-NGS-FPT IS bao gồm 24 máy được bổ sung vào các cụm cluster cụ thể như sau:

Số lượng máy chủ cơ sở dữ liệu được bổ sung như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Tên DC** | **DR\_Trans** | **DR\_Search** | **DR\_Docs** | **DC\_Ana** |
| Số lượng Node hiện tại | 48 | 54 | 46 | 30 |
| Số lượng Node bổ sung | 0 | 0 | 8 | 16 |
| Số lượng Node sau mở rộng | 48 | 54 | 54 | 46 |
| Workload | Cassandra | Search | Cassandra | Analytics + Search |

#### Mô hình tổng quan hệ thống CSDL

Dự án phục vụ mục đích mở rộng cluster HDDT nên không làm thay đổi mô hình tổng quan của hệ thống CSDL. Hệ thống vẫn bao gồm Cluster HDDT và Cluster MGMT.

Diagram, timeline

Description automatically generated

Hình 2: Mô hình tổng quan hệ thống CSDL

#### Mô hình thiết kế tại TTDL dự phòng

A diagram of a cluster

AI-generated content may be incorrect.

Sau khi được bổ sung node, cluster HDDT tại DR site sẽ bao gồm:

* 48 Node trong DR\_Trans
* 54 Node trong DR\_Search
* 54 Node trong DR\_Docs
* 46 Node trong DR\_Ana

#### Hệ thống quản trị tập trung

##### Hệ thống quản lý máy chủ vật lý

Các máy chủ được quản lý tập trung bởi giải pháp Oneview của HPE. Thông tin của máy chủ Oneview:

| **STT** | **Hostname** | **IP** | **Giao thức** | **Username** | **Password** |
| --- | --- | --- | --- | --- | --- |
|  | drm-hpeoneview | 10.64.167.238 | TCP/UDP | Administrator | \*\*\*\*\*\*\*\* |

Các cổng kết nối cần mở:

| **STT** | **Địa chỉ nguồn** | **Description** | **Địa chỉ đích** | **Description** | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 10.64.170.199-10.64.170.222 | Server ILOs | 10.64.167.238 | Oneview | 123:UDP | 1 | HPE OneView acts as an NTP server, iLO requires access. | Vĩnh viễn |
| 2 | 10.64.167.238 | Oneview | 10.64.170.199-10.64.170.222 | Server ILOs | 161:UDP | 1 | Supports SNMP GET calls to monitored and managed devices, such as, server iLO, HPE Intelligent Power Distribution Unit, and SAN Managers. | Vĩnh viễn |
| 3 | 10.64.167.238 | Oneview | 10.64.170.199-10.64.170.222 | Server ILOs | 443 | 2 | Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. | Vĩnh viễn |
| 4 | 10.64.211.11  10.64.211.14 | Management Workstation | 10.64.170.199-10.64.170.222 | Server ILOs | 443 | 1 | Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. | Vĩnh viễn |

### Thiết kế chi tiết hệ thống máy chủ Docs

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL XML được bổ sung gồm 8 node được cài đặt trên các máy chủ mật độ cao Dell PowerEdge C6620. Một Chassis Dell PowerEdge C6600 2U được lắp đặt 04 máy chủ Dell PowerEdge C6620. Mỗi máy chủ Dell PowerEdge C6620 có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data.

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 ethernet stack switch khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| Site | Trung tâm dữ liệu dự phòng |
| --- | --- |
| Tên DC​ | DR\_Docs |
| Số lượng Node bổ sung tại DC​ | 8 |
| Workload​ | Cassandra​​ |

##### Bảng phân bổ lắp đặt Rack

* Các máy chủ CSDL XML được phân bổ trên Rack vật lý như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| A11 | U12- U13 | dri-ehdxmlc6600ch15 | 1900 | 1520 | 2 | 4772.8 | 43 |
| D11 | U12- U13 | dri-ehdxmlc6600ch16 | 1900 | 1520 | 2 | 4772.8 | 43 |

* Bảng lắp đặt các máy chủ CSDL XML trên Rack chi tiết như sau:

| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| --- | --- | --- | --- | --- |
| 1 | A11 | U12- U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb135 |
| dri-ehdxmldb136 |
| dri-ehdxmldb137 |
| dri-ehdxmldb138 |
| 2 | D11 | U12- U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb139 |
| dri-ehdxmldb140 |
| dri-ehdxmldb141 |
| dri-ehdxmldb142 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A screenshot of a computer

Description automatically generated

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A computer hardware with wires connected to it

Description automatically generated with medium confidence

Hình 7: Kết nối quản trị máy chủ XML

Thông tin IP quản trị của máy chủ CSDL XML được thể hiện chị tiết qua bảng sau:

| **STT** | **Chassis** | **Hostname** | **Port Number** | **VLAN** | **IP** | **Netmask** | **Gateway** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdxmlc6600ch15 | dri-ehdxmldb135 | hwMgmt | 309 | 10.64.170.215 | 255.255.255.0 | 10.64.170.1 |
| 2 | dri-ehdxmldb136 | hwMgmt | 309 | 10.64.170.216 | 255.255.255.0 | 10.64.170.1 |
| 3 | dri-ehdxmldb137 | hwMgmt | 309 | 10.64.170.217 | 255.255.255.0 | 10.64.170.1 |
| 4 | dri-ehdxmldb138 | hwMgmt | 309 | 10.64.170.218 | 255.255.255.0 | 10.64.170.1 |
| 5 | dri-ehdxmlc6600ch16 | dri-ehdxmldb139 | hwMgmt | 309 | 10.64.170.219 | 255.255.255.0 | 10.64.170.1 |
| 6 | dri-ehdxmldb140 | hwMgmt | 309 | 10.64.170.220 | 255.255.255.0 | 10.64.170.1 |
| 7 | dri-ehdxmldb141 | hwMgmt | 309 | 10.64.170.221 | 255.255.255.0 | 10.64.170.1 |
| 8 | dri-ehdxmldb142 | hwMgmt | 309 | 10.64.170.222 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL XML được thể hiện ở bảng sau:

| **STT** | **Hostname** | **Cổng** | **VLAN** | **IP** | **Netmask** | **Gateway** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdxmldb135 | bond0 | 235 | 10.64.161.135 | 255.255.255.0 | 10.64.161.1 |
| 2 | dri-ehdxmldb136 | bond0 | 235 | 10.64.161.136 | 255.255.255.0 | 10.64.161.1 |
| 3 | dri-ehdxmldb137 | bond0 | 235 | 10.64.161.137 | 255.255.255.0 | 10.64.161.1 |
| 4 | dri-ehdxmldb138 | bond0 | 235 | 10.64.161.138 | 255.255.255.0 | 10.64.161.1 |
| 5 | dri-ehdxmldb139 | bond0 | 235 | 10.64.161.139 | 255.255.255.0 | 10.64.161.1 |
| 6 | dri-ehdxmldb140 | bond0 | 235 | 10.64.161.140 | 255.255.255.0 | 10.64.161.1 |
| 7 | dri-ehdxmldb141 | bond0 | 235 | 10.64.161.141 | 255.255.255.0 | 10.64.161.1 |
| 8 | dri-ehdxmldb142 | bond0 | 235 | 10.64.161.142 | 255.255.255.0 | 10.64.161.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL XML có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng máy như sau:

A diagram of a computer server

Description automatically generated

*Mô hình kết nối máy chủ CSDL XML*

Thông tin chi tiết kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | |  |  |  | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb135 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/18 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb135 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/7 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb135 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb136 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/19 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb136 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/8 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb136 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb137 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/20 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb137 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/9 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb137 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb138 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/21 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb138 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/10 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U12-U13 | dri-ehdxmlc6600ch15 | dri-ehdxmldb138 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb139 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/22 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb139 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/11 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb139 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb140 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/23 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb140 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/12 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb140 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb141 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/24 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb141 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/13 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb141 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb142 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/25 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb142 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/14 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U12-U13 | dri-ehdxmlc6600ch16 | dri-ehdxmldb142 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Docs

Bảng thông số các máy chủ CSDL Docs như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (TB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdxmldb135 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.135 |
| 2 | dri-ehdxmldb136 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.136 |
| 3 | dri-ehdxmldb137 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.137 |
| 4 | dri-ehdxmldb138 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.138 |
| 5 | dri-ehdxmldb139 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.139 |
| 6 | dri-ehdxmldb140 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.140 |
| 7 | dri-ehdxmldb141 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.141 |
| 8 | dri-ehdxmldb142 | RHEL 8.10 | 24 | 128 | 4 x 1.92 | 10.64.161.142 |

Các máy chủ sẽ được cấu hình thiết lập các thông số theo chính sách của TCT như sau:

|  |  |
| --- | --- |
| **Thông số** | **Giá trị** |
| DNS Server | 10.64.89.11  10.64.89.13 |
| NTP Server | 10.64.68.26  10.64.68.27  10.64.68.32 |
| Virtualization Technology | Enable |
| Hyper-Threading | Enable |
| CPU frequency scaling | Disable |
| zone\_reclaim\_mode | Disable |
| swap | Disable |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ monitor, debug, khác | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:
* Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.
* HĐH của máy chủ sẽ được ưu tiên về tốc độ xử lý. Do đó HĐH sẽ được cài đặt lưu trên RAID0 Array tạo từ 01 ổ cứng.
* Với phân vùng data, dữ liệu sẽ được lưu trên các ổ cứng không tạo RAID. Trên HĐH sẽ sử dụng LVM để gộp thành 03 ổ cứng Non-RAID này thành 1 ổ logic.
* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 1.92 TB (RAID 0) | sda | sdd1 | 600 MiB | - | - | /boot/efi | efi |  |
| sdd2 | 1 GiB | - | - | /boot | xfs |  |
| sdd3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sdd4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sdd5 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 1550 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 1.92 TB (No Raid) | sda | sda1 | 5.238 TiB | vg\_data | lv\_data | /data | xfs |  |
| 3 | 01 x 1.92 TB (No Raid) | sdb | sdb1 |
| 4 | 01 x 1.92 TB (No Raid) | sdc | sdc1 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

| **Thông số** | **Value** |
| --- | --- |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các tham số khác:

| **Tham số** | **Giá trị** | **Chú thích** |
| --- | --- | --- |
| Disable CPU frequency scaling | for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done | Disable CPU frequency scaling |
| zone\_reclaim\_mode | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab  sudo swapoff –all | Disable swap |
| Optimize SSDs |  |  |
| /sys/block/device\_name/queue/schedu | deadline | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| /sys/block/device\_name/queue/nr\_requests | 128 | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| /sys/class/block/device\_name/queue/rotational | 0 |  |
| /sys/class/block/device\_name/queue/read\_ahead\_kb | 8 |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Thông số User và CSDL

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| hddt\_adhoc | hddt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng HDDT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| hddt\_app | hddt\_app | ks\_hddt\_system.hddt\_service\_config | SELECT |
| hddt\_category | hddt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_hddt\_system ks\_dangky | SELECT, UPDATE |
| hddt\_config | hddt\_config | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_delegation | hddt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_examination | hddt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| hddt\_explanation | hddt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| hddt\_explanation\_tvan | hddt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice | hddt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice\_code | hddt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| hddt\_invoice\_code\_adhoc | hddt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| hddt\_job | hddt\_job | ks\_hddt\_system | SELECT |
| hddt\_job\_config | hddt\_job\_config | ks\_hddt\_system ks\_danhmuc | SELECT, UPDATE |
| hddt\_message | hddt\_message | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_query | hddt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration | hddt\_registration | ks\_hddt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration\_status | hddt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| hddt\_security\_official | hddt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_security\_taxpayer | hddt\_security\_taxpayer | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_sync | hddt\_sync | ks\_danhmuc | SELECT, UPDATE |
| hddt\_system | hddt\_system | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_tax\_risk | hddt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_expired | hddt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_status | hddt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tvan\_status | hddt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_verification | hddt\_verification | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_hddt\_to\_dwh\_ods | job\_hddt\_to\_dwh\_ods | ks\_dangky.hddt\_dky  ks\_dangky.hddt\_tkhai  ks\_hoadon.hddt\_bthctiet\_mgr  ks\_hoadon.hddt\_bthop  ks\_hoadon.hddt\_hdhhdvu  ks\_hoadon.hddt\_hdon  ks\_hoadon.hddt\_tbhgthdon  ks\_hoadon.hddt\_tbssdt  ks\_hosogoc.hddt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_hddt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
| 2 | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 8443, 8888, 61620 :TCP | 1 | Mở cổng từ các DSE node đến máy chủ quản trị DSE OpsCenter | Vĩnh viễn |
| 3 | 10.64.211.14,  10.64.211.12, 10.64.211.11 | Máy chủ Terminal | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 22,4040,5598,5599,7080,7081,8983,9042,9142,9091,9077,9999,18080:TCP | 1 | Mở cổng từ Remote client tới các DSE node | Vĩnh viễn |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 | Dashboard Grafana | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.212.206 => 10.64.212.208 | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP) | HDDT Core Microservice | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Docs | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Docs | Vĩnh viễn |
| 3 | 10.64.90.153 => 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Docs | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.161.135=> 10.64.161.142 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.102.101 => 10.64.102.129 ,  10.64.102.131 => 10.64.102.159 ,  10.64.102.161 => 10.64.102.191 ,  10.64.161.11 => 10.64.161.17,  10.64.161.22 => 10.64.161.52 | DSE (DC\_Docs, DR\_Docs) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ XML cũ sang các máy chủ XML mới | Vĩnh viễn |

#### Thông số chi tiết CSDL DOC

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Loại** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| Security | client\_encryption\_options | enabled TRUE |
| General | num\_tokens | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | 3 |
| tpc\_pending\_requests\_limit | 256 |
| tpc\_cores |  |
| Directory | data\_file\_directories | /data/data |
| commitlog\_directory | /commitlog |
| saved\_caches\_directory | /data/saved\_caches |
| Ports | native\_transport\_port\_ssl | 9142 |
| NodeSync | rate\_in\_kb | 10240 |
| Caches | row\_cache\_size\_in\_mb | 500 |
| row\_cache\_save\_period | 36000 |
| Timeouts | read\_request\_timeout\_in\_ms | 5000 |
| write\_request\_timeout\_in\_ms | 2000 |
| stream\_outbound\_permits\_in\_mb | 8 |
| input\_stream\_channel\_timeout\_in\_ms | 432000000 |
| Snapshots | incremental\_backups | TRUE |
| auto\_snapshot | TRUE |
| Hinted Handoff | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hints\_delivery\_threads | 6 |
| hints\_directory | /data/hints |
| Change Data Capture | cdc\_raw\_directory | /data/cdc\_raw |
| Miscellaneous | metadata\_directory | /data/metadata |
| Cluster Communication | endpoint\_snitch | GossipingPropertyFileSnitch |
| zerocopy\_streaming\_enabled | FALSE |

* Thông số File dse.yaml:

| **Loại** | **Tham số** | **Tham số thành phần** | **Giá trị** |
| --- | --- | --- | --- |
| DSE Authorizer Options | authorization\_options | enabled | TRUE |
| transitional\_mode | disabled |
| allow\_row\_level\_security | FALSE |
| DSE Metrics Collector | insights\_options | data\_dir | /data/insights |
| log\_dir | /u01/log/dse/insights |
| Encryption Settings | system\_key\_directory |  | /u01/app/dse/conf |
| Audit Logging Settings | audit\_logging\_options | enabled | TRUE |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| Miscellaneous | internode\_messaging\_options | client\_max\_connections | 200 |
| port | 8609 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

|  |  |  |
| --- | --- | --- |
| **THAM SỐ DR\_DOC** | | |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_DOC |  |
| Số lượng Node bổ sung | 8 |  |
| Workload | Cassandra |  |

##### Thông số Logical Rack

Logical Rack của DR\_Doc được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 02 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Doc:
* Số lượng node: 8
* Logical rack: 02
* Số lượng nodes trên logical rack dr\_doc1: 4
* Số lượng nodes trên logical rack dr\_doc2: 4
* Thông tin được hiển thị chi tiết theo bảng sau:

| **TT** | **DC** | **Tham số** | **Physical Rack** | | **Tổng** |
| --- | --- | --- | --- | --- | --- |
| **Rack A11** | **Rack D11** |
| 1 | DR\_Doc 8 node (RF=2) | Chassis | 1 | 1 | 2 |
| Nodes | 4 | 4 | 8 |
| Logical Rack ID | dr\_doc1 | dr\_doc2 |  |

##### Thông số các Node CSDL DOC

Thông số cấu hình từng node CSDL XML như sau:

| **CẤU HÌNH TỪNG NODE XML** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 x 1.92TB (SSD) |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 5.2TiB |  |
| DNS | 10.64.89.11 |  |
| 10.64.89.13 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Doc

| **THÔNG TIN CÁC KEYSPACE ỨNG DỤNG** | | |
| --- | --- | --- |
| **Tên keyspace** | **Chú thích** | **Keyspace replication Strategy** |
| ks\_hosogoc  (Hồ sơ gốc) | Phục vụ mục đích tra cứu thông tin hồ sơ gốc như: Tờ khai đăng ký, Thông báo, Hóa đơn gốc từ NNT gửi cho CQT. | NetworkTopologyStrategy |
| OpsCenter | Quản trị OpsCenter | NetworkTopologyStrategy |
| ks\_kad (Kafka) | Quản trị Kafka | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Doc, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Doc được phân bố theo bảng sau:

| **THÔNG TIN CÁC KEYSPACE ỨNG DỤNG** | | |
| --- | --- | --- |
| **Tên keyspace** | **Chú thích** | **Keyspace replication Strategy** |
| ks\_hosogoc  (Hồ sơ gốc) | Phục vụ mục đích tra cứu thông tin hồ sơ gốc như: Tờ khai đăng ký, Thông báo, Hóa đơn gốc từ NNT gửi cho CQT. | NetworkTopologyStrategy |
| OpsCenter | Quản trị OpsCenter | NetworkTopologyStrategy |
| ks\_kad (Kafka) | Quản trị Kafka | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL DOC tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 10 phút kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Mỗi máy chủ được cấu hình log với dung lượng không quá 500Mb hoặc thời gian lưu trữ không quá 6 tháng.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.158 | 9997 |
| 10.64.212.159 | 9997 |
| 10.64.212.213 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.215 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |

### Thiết kế chi tiết hệ thống máy chủ Ana

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL Ana được bổ sung gồm 16 node được cài đặt trên các máy chủ mật độ cao Dell PowerEdge C6620. Một Chassis Dell PowerEdge C6600 2U được lắp đặt 04 máy chủ Dell PowerEdge C6620. Mỗi máy chủ Dell PowerEdge C6620 có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data.

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 ethernet stack switch khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| Site | Trung tâm dữ liệu dự phòng |
| --- | --- |
| Tên DC​ | DR\_Ana |
| Số lượng Node bổ sung tại DC​ | 16 |
| Workload​ | Analytics + Search ​​ |

##### Bảng phân bổ lắp đặt Rack

* Các máy chủ CSDL Ana được phân bổ trên Rack vật lý như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chasiss** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| A11 | U15-U16 | dri-ehdanac6600ch10 | 1900 | 1520 | 2 | 4772.8 | 43 |
| A11 | U17-U18 | dri-ehdanac6600ch11 | 1900 | 1520 | 2 | 4772.8 | 43 |
| D11 | U15-U16 | dri-ehdanac6600ch12 | 1900 | 1520 | 2 | 4772.8 | 43 |
| D11 | U17-U18 | dri-ehdanac6600ch13 | 1900 | 1520 | 2 | 4772.8 | 43 |

* Bảng lắp đặt các máy chủ CSDL XML trên Rack chi tiết như sau:

| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| --- | --- | --- | --- | --- |
| 1 | A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb172 |
| dri-ehdanadb173 |
| dri-ehdanadb174 |
| dri-ehdanadb175 |
| 2 | A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb176 |
| dri-ehdanadb177 |
| dri-ehdanadb178 |
| dri-ehdanadb179 |
| 3 | D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb180 |
| dri-ehdanadb181 |
| dri-ehdanadb182 |
| dri-ehdanadb183 |
| 4 | D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb184 |
| dri-ehdanadb185 |
| dri-ehdanadb186 |
| dri-ehdanadb187 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A table of information with numbers and letters

Description automatically generated with medium confidence

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A diagram of a computer server

Description automatically generated

Hình 8: Kết nối quản trị máy chủ Ana

Thông tin IP quản trị của máy chủ CSDL Ana được thể hiện chị tiết qua bảng sau:

| **No.** | **Chassis** | **Device** | **VLAN** | **IP iDRAC** | **Netmask** | **GateWay** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdanac6600ch10 | dri-ehdanadb172 | 309 | 10.64.170.199 | 255.255.255.0 | 10.64.170.1 |
| 2 |  | dri-ehdanadb173 | 309 | 10.64.170.200 | 255.255.255.0 | 10.64.170.1 |
| 3 |  | dri-ehdanadb174 | 309 | 10.64.170.201 | 255.255.255.0 | 10.64.170.1 |
| 4 |  | dri-ehdanadb175 | 309 | 10.64.170.202 | 255.255.255.0 | 10.64.170.1 |
| 5 | dri-ehdanac6600ch11 | dri-ehdanadb176 | 309 | 10.64.170.203 | 255.255.255.0 | 10.64.170.1 |
| 6 |  | dri-ehdanadb177 | 309 | 10.64.170.204 | 255.255.255.0 | 10.64.170.1 |
| 7 |  | dri-ehdanadb178 | 309 | 10.64.170.205 | 255.255.255.0 | 10.64.170.1 |
| 8 |  | dri-ehdanadb179 | 309 | 10.64.170.206 | 255.255.255.0 | 10.64.170.1 |
| 9 | dri-ehdanac6600ch12 | dri-ehdanadb180 | 309 | 10.64.170.207 | 255.255.255.0 | 10.64.170.1 |
| 10 |  | dri-ehdanadb181 | 309 | 10.64.170.208 | 255.255.255.0 | 10.64.170.1 |
| 11 |  | dri-ehdanadb182 | 309 | 10.64.170.209 | 255.255.255.0 | 10.64.170.1 |
| 12 |  | dri-ehdanadb183 | 309 | 10.64.170.210 | 255.255.255.0 | 10.64.170.1 |
| 13 | dri-ehdanac6600ch13 | dri-ehdanadb184 | 309 | 10.64.170.211 | 255.255.255.0 | 10.64.170.1 |
| 14 |  | dri-ehdanadb185 | 309 | 10.64.170.212 | 255.255.255.0 | 10.64.170.1 |
| 15 |  | dri-ehdanadb186 | 309 | 10.64.170.213 | 255.255.255.0 | 10.64.170.1 |
| 16 |  | dri-ehdanadb187 | 309 | 10.64.170.214 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL Ana được thể hiện ở bảng sau:

| **No.** | **Chassis** | **Device** | **VLAN** | **IP Data** | **Netmask** | **GateWay** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdanac6600ch10 | dri-ehdanadb172 | 234 | 10.64.160.172 | 255.255.255.0 | 10.64.160.1 |
| 2 |  | dri-ehdanadb173 | 234 | 10.64.160.173 | 255.255.255.0 | 10.64.160.1 |
| 3 |  | dri-ehdanadb174 | 234 | 10.64.160.174 | 255.255.255.0 | 10.64.160.1 |
| 4 |  | dri-ehdanadb175 | 234 | 10.64.160.175 | 255.255.255.0 | 10.64.160.1 |
| 5 | dri-ehdanac6600ch11 | dri-ehdanadb176 | 234 | 10.64.160.176 | 255.255.255.0 | 10.64.160.1 |
| 6 |  | dri-ehdanadb177 | 234 | 10.64.160.177 | 255.255.255.0 | 10.64.160.1 |
| 7 |  | dri-ehdanadb178 | 234 | 10.64.160.178 | 255.255.255.0 | 10.64.160.1 |
| 8 |  | dri-ehdanadb179 | 234 | 10.64.160.179 | 255.255.255.0 | 10.64.160.1 |
| 9 | dri-ehdanac6600ch12 | dri-ehdanadb180 | 234 | 10.64.160.180 | 255.255.255.0 | 10.64.160.1 |
| 10 |  | dri-ehdanadb181 | 234 | 10.64.160.181 | 255.255.255.0 | 10.64.160.1 |
| 11 |  | dri-ehdanadb182 | 234 | 10.64.160.182 | 255.255.255.0 | 10.64.160.1 |
| 12 |  | dri-ehdanadb183 | 234 | 10.64.160.183 | 255.255.255.0 | 10.64.160.1 |
| 13 | dri-ehdanac6600ch13 | dri-ehdanadb184 | 234 | 10.64.160.184 | 255.255.255.0 | 10.64.160.1 |
| 14 |  | dri-ehdanadb185 | 234 | 10.64.160.185 | 255.255.255.0 | 10.64.160.1 |
| 15 |  | dri-ehdanadb186 | 234 | 10.64.160.186 | 255.255.255.0 | 10.64.160.1 |
| 16 |  | dri-ehdanadb187 | 234 | 10.64.160.187 | 255.255.255.0 | 10.64.160.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL ANA có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng máy như sau:

A diagram of a computer server

Description automatically generated

*Mô hình kết nối máy chủ CSDL ANA*

Thông tin chi tiết kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | |  |  |  | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb172 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/34 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb172 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/21 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb172 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb173 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/35 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb173 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/22 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb173 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb174 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/36 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb174 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/23 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb174 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb175 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/37 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb175 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/24 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U15-U16 | dri-ehdanac6600ch10 | dri-ehdanadb175 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb176 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/38 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb176 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/25 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb176 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb177 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/39 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb177 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/26 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb177 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb178 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/40 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb178 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/27 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb178 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb179 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/41 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb179 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/28 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U17-U18 | dri-ehdanac6600ch11 | dri-ehdanadb179 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb180 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/42 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb180 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/29 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb180 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb181 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/43 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb181 | P1 | Active | bond0 | D01 | U31 | DR-INT-ACCSW-11 | Eth1/30 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb181 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb182 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/44 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb182 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/1 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb182 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb183 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/45 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb183 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/2 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U15-U16 | dri-ehdanac6600ch12 | dri-ehdanadb183 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb184 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/46 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb184 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/3 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb184 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb185 | iDRAC |  |  | A01 | U39 | DR-MGMT-ACCSW07 | ge-0/0/47 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb185 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/4 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb185 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb186 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/16 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb186 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/5 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb186 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb187 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/17 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U17-U18 | dri-ehdanac6600ch13 | dri-ehdanadb187 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/6 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U17-U18 | dri-ehdanac6600c13 | dri-ehdanadb187 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Ana

Bảng thông số các máy chủ CSDL Ana như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (GB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdanadb172 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.172 |
| 2 | dri-ehdanadb173 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.173 |
| 3 | dri-ehdanadb174 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.174 |
| 4 | dri-ehdanadb175 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.175 |
| 5 | dri-ehdanadb176 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.176 |
| 6 | dri-ehdanadb177 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.177 |
| 7 | dri-ehdanadb178 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.178 |
| 8 | dri-ehdanadb179 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.179 |
| 9 | dri-ehdanadb180 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.180 |
| 10 | dri-ehdanadb181 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.181 |
| 11 | dri-ehdanadb182 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.182 |
| 12 | dri-ehdanadb183 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.183 |
| 13 | dri-ehdanadb184 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.184 |
| 14 | dri-ehdanadb185 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.185 |
| 15 | dri-ehdanadb186 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.186 |
| 16 | dri-ehdanadb187 | RHEL 8.10 | 24 | 128 | 4 x 960 | 10.64.160.187 |

Thông số cấu hình các dịch vụ mạng

|  |  |
| --- | --- |
| DNS Server | 10.64.88.11, 10.64.88.12 |
| NTP Server | 10.64.68.26 |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ monitor, debug, khác | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:
* Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.
* HĐH của máy chủ sẽ được ưu tiên về tốc độ xử lý. Do đó HĐH sẽ được cài đặt lưu trên RAID0 Array tạo từ 01 ổ cứng.
* Với phân vùng solr\_index, trên HĐH sẽ cài đặt để lưu trên 01 ổ cứng Non-RAID.
* Với phân vùng data, dữ liệu sẽ được lưu trên các ổ cứng không tạo RAID. Trên HĐH sẽ sử dụng LVM để gộp thành 02 ổ cứng Non-RAID này thành 1 ổ logic.
* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 960 GB (RAID 0) | sda | sda1 | 600 MiB | - | - | /boot/efi | efi |  |
| sda2 | 1 GiB | - | - | /boot | xfs |  |
| sda3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sda4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sda6 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 664 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 960 GB (No Raid) | sdb | sdb1 | 650 GiB | vg\_solr | lv\_solr | /solr\_index | xfs |  |
| Free | 224 GiB |  |  |  |  | dự phòng |
| 3 | 01 x 960 GB (No Raid) | sdc | sdc1 | 1.746 TiB | vg\_data | lv\_data | /data | xfs |  |
| 4 | 01 x 960 GB (No Raid) | sdd | sdd1 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

| **Thông số** | **Value** |
| --- | --- |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các thm số khác:

| **Tham số** | **Giá trị** | **Chú thích** |
| --- | --- | --- |
| Disable CPU frequency scaling | for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done | Disable CPU frequency scaling |
| zone\_reclaim\_mode | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab  sudo swapoff –all | Disable swap |
| Optimize SSDs |  |  |
| /sys/block/device\_name/queue/schedu | deadline | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| /sys/block/device\_name/queue/nr\_requests | 128 | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| /sys/class/block/device\_name/queue/rotational | 0 |  |
| /sys/class/block/device\_name/queue/read\_ahead\_kb | 8 |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Thông số User và CSDL Ana

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| hddt\_adhoc | hddt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng HDDT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| hddt\_app | hddt\_app | ks\_hddt\_system.hddt\_service\_config | SELECT |
| hddt\_category | hddt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_hddt\_system ks\_dangky | SELECT, UPDATE |
| hddt\_config | hddt\_config | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_delegation | hddt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_examination | hddt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| hddt\_explanation | hddt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| hddt\_explanation\_tvan | hddt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice | hddt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice\_code | hddt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| hddt\_invoice\_code\_adhoc | hddt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| hddt\_job | hddt\_job | ks\_hddt\_system | SELECT |
| hddt\_job\_config | hddt\_job\_config | ks\_hddt\_system ks\_danhmuc | SELECT, UPDATE |
| hddt\_message | hddt\_message | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_query | hddt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration | hddt\_registration | ks\_hddt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration\_status | hddt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| hddt\_security\_official | hddt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_security\_taxpayer | hddt\_security\_taxpayer | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_sync | hddt\_sync | ks\_danhmuc | SELECT, UPDATE |
| hddt\_system | hddt\_system | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_tax\_risk | hddt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_expired | hddt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_status | hddt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tvan\_status | hddt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_verification | hddt\_verification | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_hddt\_to\_dwh\_ods | job\_hddt\_to\_dwh\_ods | ks\_dangky.hddt\_dky  ks\_dangky.hddt\_tkhai  ks\_hoadon.hddt\_bthctiet\_mgr  ks\_hoadon.hddt\_bthop  ks\_hoadon.hddt\_hdhhdvu  ks\_hoadon.hddt\_hdon  ks\_hoadon.hddt\_tbhgthdon  ks\_hoadon.hddt\_tbssdt  ks\_hosogoc.hddt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_hddt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
| 2 | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 8443, 8888, 61620 :TCP | 1 | Mở cổng từ các DSE node đến máy chủ quản trị DSE OpsCenter | Vĩnh viễn |
| 3 | 10.64.211.14,  10.64.211.12, 10.64.211.11 | Máy chủ Terminal | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 22,4040,5598,5599,7080,7081,8983,9042,9142,9091,9077,9999,18080:TCP | 1 | Mở cổng từ Remote client tới các DSE node | Vĩnh viễn |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 | Dashboard Grafana | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 10.64.212.206 => 10.64.212.208 | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP) | HDDT Core Microservice | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Docs | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Docs | Vĩnh viễn |
| 3 | 10.64.90.153 => 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Docs | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.160.172=> 10.64.160.187 | Máy chủ DSE Ana mới (DR\_Ana) | 10.64.101.11=> 10.64.101.75,  10.64.160.11 => 10.64.160.40 | DSE (DC\_Ana, DR\_Ana) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ XML cũ sang các máy chủ XML mới | Vĩnh viễn |

#### Thông số chi tiết CSDL Ana

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Tên tham số** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| permissions\_cache\_max\_entries | permissions\_cache\_max\_entries | 1000 |
| ssl\_storage\_port | ssl\_storage\_port | 7001 |
| guardrails | guardrails |  |
| batch\_size\_fail\_threshold\_in\_kb | 640 |
| tombstone\_warn\_threshold | 1000 |
| tombstone\_failure\_threshold | 100000 |
| disk\_usage\_max\_disk\_size\_in\_gb | -1 |
| batch\_size\_warn\_threshold\_in\_kb | 64 |
| partition\_size\_warn\_threshold\_in\_mb | 100 |
| storage\_port | storage\_port | 7000 |
| backup\_service | backup\_service |  |
| enabled | FALSE |
| continuous\_paging | continuous\_paging |  |
| max\_concurrent\_sessions | 240 |
| max\_session\_pages | 4 |
| max\_page\_size\_mb | 8 |
| max\_local\_query\_time\_ms | 5000 |
| client\_timeout\_sec | 600 |
| cancel\_timeout\_sec | 5 |
| paused\_check\_interval\_ms | 1 |
| batchlog\_replay\_throttle\_in\_kb | batchlog\_replay\_throttle\_in\_kb | 1024 |
| commit\_failure\_policy | commit\_failure\_policy | stop |
| native\_transport\_max\_frame\_size\_in\_mb | native\_transport\_max\_frame\_size\_in\_mb | 256 |
| commitlog\_segment\_size\_in\_mb | commitlog\_segment\_size\_in\_mb | 32 |
| memtable\_flush\_writers | memtable\_flush\_writers | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | allocate\_tokens\_for\_local\_replication\_factor | 2 |
| client\_encryption\_options | client\_encryption\_options |  |
| truststore | /etc/dse/keystores/client.truststore |
| protocol | TLS |
| optional | FALSE |
| require\_client\_auth | FALSE |
| enabled | TRUE |
| truststore\_password | cassandra |
| algorithm | SunX509 |
| keystore | /etc/dse/keystores/client.keystore |
| truststore\_type | JKS |
| keystore\_type | JKS |
| keystore\_password | cassandra |
| inter\_dc\_tcp\_nodelay | inter\_dc\_tcp\_nodelay | FALSE |
| column\_index\_cache\_size\_in\_kb | column\_index\_cache\_size\_in\_kb | 2 |
| internode\_authenticator | internode\_authenticator | org.apache.cassandra.auth.AllowAllInternodeAuthenticator |
| max\_value\_size\_in\_mb | max\_value\_size\_in\_mb | 256 |
| authorizer | authorizer | com.datastax.bdp.cassandra.auth.DseAuthorizer |
| num\_tokens | num\_tokens | 8 |
| listen\_on\_broadcast\_address | listen\_on\_broadcast\_address | FALSE |
| row\_cache\_save\_period | row\_cache\_save\_period | 36000 |
| row\_cache\_class\_name | row\_cache\_class\_name | org.apache.cassandra.cache.OHCProvider |
| native\_transport\_allow\_older\_protocols | native\_transport\_allow\_older\_protocols | TRUE |
| disk\_failure\_policy | disk\_failure\_policy | stop |
| native\_transport\_port | native\_transport\_port | 9042 |
| enable\_user\_defined\_functions\_threads | enable\_user\_defined\_functions\_threads | TRUE |
| server\_encryption\_options | server\_encryption\_options |  |
| internode\_encryption | none |
| dynamic\_snitch\_reset\_interval\_in\_ms | dynamic\_snitch\_reset\_interval\_in\_ms | 600000 |
| compaction\_throughput\_mb\_per\_sec | compaction\_throughput\_mb\_per\_sec | 64 |
| data\_file\_directories | data\_file\_directories | /data/data |
| role\_manager | role\_manager | com.datastax.bdp.cassandra.auth.DseRoleManager |
| leaks\_detection\_params | leaks\_detection\_params |  |
| sampling\_probability | 0,01 |
| max\_stacks\_cache\_size\_mb | 32 |
| num\_access\_records | 0 |
| max\_stack\_depth | 30 |
| column\_index\_size\_in\_kb | column\_index\_size\_in\_kb | 16 |
| windows\_timer\_interval | windows\_timer\_interval | 1 |
| rpc\_keepalive | rpc\_keepalive | TRUE |
| commitlog\_total\_space\_in\_mb | commitlog\_total\_space\_in\_mb | 8192 |
| nodesync | nodesync |  |
| rate\_in\_kb | 10240 |
| snapshot\_before\_compaction | snapshot\_before\_compaction | FALSE |
| tracetype\_query\_ttl | tracetype\_query\_ttl | 86400 |
| native\_transport\_port\_ssl | native\_transport\_port\_ssl | 9142 |
| pick\_level\_on\_streaming | pick\_level\_on\_streaming | TRUE |
| system\_keyspaces\_filtering | system\_keyspaces\_filtering | FALSE |
| row\_cache\_size\_in\_mb | row\_cache\_size\_in\_mb | 500 |
| tracetype\_repair\_ttl | tracetype\_repair\_ttl | 604800 |
| auto\_bootstrap | auto\_bootstrap | TRUE |
| commitlog\_sync | commitlog\_sync | periodic |
| concurrent\_validations | concurrent\_validations | 0 |
| disk\_optimization\_strategy | disk\_optimization\_strategy | ssd |
| counter\_cache\_save\_period | counter\_cache\_save\_period | 7200 |
| emulate\_dbaas\_defaults | emulate\_dbaas\_defaults | FALSE |
| user\_defined\_function\_warn\_micros | user\_defined\_function\_warn\_micros | 500 |
| back\_pressure\_enabled | back\_pressure\_enabled | FALSE |
| user\_defined\_function\_fail\_micros | user\_defined\_function\_fail\_micros | 10000 |
| slow\_query\_log\_timeout\_in\_ms | slow\_query\_log\_timeout\_in\_ms | 500 |
| trickle\_fsync | trickle\_fsync | TRUE |
| streaming\_keep\_alive\_period\_in\_secs | streaming\_keep\_alive\_period\_in\_secs | 300 |
| io\_global\_queue\_depth | io\_global\_queue\_depth | 128 |
| write\_request\_timeout\_in\_ms | write\_request\_timeout\_in\_ms | 2000 |
| initial\_token | initial\_token | null |
| incremental\_backups | incremental\_backups | TRUE |
| truncate\_request\_timeout\_in\_ms | truncate\_request\_timeout\_in\_ms | 60000 |
| snapshot\_before\_dropping\_column | snapshot\_before\_dropping\_column | FALSE |
| enable\_scripted\_user\_defined\_functions | enable\_scripted\_user\_defined\_functions | FALSE |
| read\_request\_timeout\_in\_ms | read\_request\_timeout\_in\_ms | 5000 |
| request\_timeout\_in\_ms | request\_timeout\_in\_ms | 10000 |
| start\_native\_transport | start\_native\_transport | TRUE |
| back\_pressure\_strategy | back\_pressure\_strategy |  |
| - class\_name | org.apache.cassandra.net.RateBasedBackPressure |
| parameters |  |
| - high\_ratio | 0,9 |
| factor | 5 |
| flow | FAST |
| metadata\_directory | metadata\_directory | /data/metadata |
| concurrent\_materialized\_view\_builders | concurrent\_materialized\_view\_builders | 2 |
| memtable\_allocation\_type | memtable\_allocation\_type | offheap\_objects |
| saved\_caches\_directory | saved\_caches\_directory | /data/saved\_caches |
| transparent\_data\_encryption\_options | transparent\_data\_encryption\_options |  |
| enabled | FALSE |
| chunk\_length\_kb | 64 |
| cipher | AES/CBC/PKCS5Padding |
| key\_alias | testing:1 |
| internode\_compression | internode\_compression | dc |
| authenticator | authenticator | com.datastax.bdp.cassandra.auth.DseAuthenticator |
| phi\_convict\_threshold | phi\_convict\_threshold | 8 |
| max\_hints\_delivery\_threads | max\_hints\_delivery\_threads | 6 |
| cross\_node\_timeout | cross\_node\_timeout | FALSE |
| partitioner | partitioner | org.apache.cassandra.dht.Murmur3Partitioner |
| max\_pending\_lw\_transactions | max\_pending\_lw\_transactions | 10000 |
| hinted\_handoff\_enabled | hinted\_handoff\_enabled | TRUE |
| hints\_flush\_period\_in\_ms | hints\_flush\_period\_in\_ms | 10000 |
| enable\_user\_defined\_functions | enable\_user\_defined\_functions | FALSE |
| hinted\_handoff\_throttle\_in\_kb | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hint\_window\_in\_ms | max\_hint\_window\_in\_ms | 10800000 |
| otc\_coalescing\_strategy | otc\_coalescing\_strategy | DISABLED |
| user\_defined\_function\_warn\_heap\_mb | user\_defined\_function\_warn\_heap\_mb | 200 |
| auto\_snapshot | auto\_snapshot | TRUE |
| cdc\_raw\_directory | cdc\_raw\_directory | /data/cdc\_raw |
| range\_request\_timeout\_in\_ms | range\_request\_timeout\_in\_ms | 10000 |
| user\_function\_timeout\_policy | user\_function\_timeout\_policy | die |
| stream\_throughput\_outbound\_megabits\_per\_sec | stream\_throughput\_outbound\_megabits\_per\_sec | 200 |
| commitlog\_directory | commitlog\_directory | /commitlog |
| sstable\_preemptive\_open\_interval\_in\_mb | sstable\_preemptive\_open\_interval\_in\_mb | 50 |
| seed\_provider | seed\_provider |  |
| - class\_name | org.apache.cassandra.locator.SimpleSeedProvider |
| parameters |  |
| - seeds | 10.64.99.117, 10.64.101.18, 10.64.160.25, 10.64.159.11, 10.64.161.34, 10.64.158.19,10.64.102.101, 10.64.158.11, 10.64.100.111, 10.64.99.133, 10.64.100.121, 10.64.161.22,10.64.101.37, 10.64.100.101, 10.64.102.161, 10.64.159.29, 10.64.160.11, 10.64.159.25,10.64.99.101, 10.64.158.25, 10.64.161.11, 10.64.160.18, 10.64.102.131, 10.64.101.11 |
| dynamic\_snitch\_update\_interval\_in\_ms | dynamic\_snitch\_update\_interval\_in\_ms | 100 |
| trickle\_fsync\_interval\_in\_kb | trickle\_fsync\_interval\_in\_kb | 10240 |
| commitlog\_sync\_period\_in\_ms | commitlog\_sync\_period\_in\_ms | 10000 |
| cdc\_enabled | cdc\_enabled | FALSE |
| max\_hints\_file\_size\_in\_mb | max\_hints\_file\_size\_in\_mb | 128 |
| counter\_write\_request\_timeout\_in\_ms | counter\_write\_request\_timeout\_in\_ms | 5000 |
| zerocopy\_streaming\_enabled | zerocopy\_streaming\_enabled | FALSE |
| cluster\_name | cluster\_name | HDDT |
| zerocopy\_max\_sstables | zerocopy\_max\_sstables | ? |
| endpoint\_snitch | endpoint\_snitch | GossipingPropertyFileSnitch |
| cross\_dc\_rtt\_in\_ms | cross\_dc\_rtt\_in\_ms | 0 |
| streaming\_connections\_per\_host | streaming\_connections\_per\_host | 1 |
| hints\_directory | hints\_directory | /data/hints |
| dynamic\_snitch\_badness\_threshold | dynamic\_snitch\_badness\_threshold | 0,1 |
| concurrent\_lw\_transactions | concurrent\_lw\_transactions | 128 |
| native\_transport\_max\_concurrent\_connections\_per\_ip | native\_transport\_max\_concurrent\_connections\_per\_ip | -1 |
| user\_defined\_function\_fail\_heap\_mb | user\_defined\_function\_fail\_heap\_mb | 500 |
| permissions\_validity\_in\_ms | permissions\_validity\_in\_ms | 1200000 |
| roles\_validity\_in\_ms | roles\_validity\_in\_ms | 1200000 |
| cas\_contention\_timeout\_in\_ms | cas\_contention\_timeout\_in\_ms | 1000 |
| seed\_gossip\_probability | seed\_gossip\_probability | 1 |
| zerocopy\_max\_unused\_metadata\_in\_mb | zerocopy\_max\_unused\_metadata\_in\_mb | ? |
| native\_transport\_max\_concurrent\_connections | native\_transport\_max\_concurrent\_connections | -1 |
| aggregated\_request\_timeout\_in\_ms | aggregated\_request\_timeout\_in\_ms | 120000 |

* Thông số File dse.yaml:

| **Dạng tham số** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| spark\_cluster\_info\_options | spark\_cluster\_info\_options |  |
| enabled | false |
| system\_info\_encryption | system\_info\_encryption |  |
| enabled | false |
| authentication\_options | authentication\_options |  |
| enabled | true |
| default\_scheme | internal |
| other\_schemes | [] |
| scheme\_permissions | false |
| allow\_digest\_with\_kerberos | true |
| plain\_text\_without\_ssl | warn |
| transitional\_mode | disabled |
| spark\_security\_enabled | spark\_security\_enabled | false |
| config\_encryption\_active | config\_encryption\_active | false |
| histogram\_data\_options | histogram\_data\_options |  |
| enabled | false |
| performance\_queue\_capacity | performance\_queue\_capacity | 32000 |
| spark\_security\_encryption\_enabled | spark\_security\_encryption\_enabled | false |
| spark\_process\_runner | spark\_process\_runner |  |
| runner\_type | default |
| run\_as\_runner\_options |  |
| user\_slots |  |
| - slot1 | - slot1 |
| - slot2 | - slot2 |
| solr\_resource\_upload\_limit\_mb | solr\_resource\_upload\_limit\_mb | 10 |
| resource\_level\_latency\_tracking\_options | resource\_level\_latency\_tracking\_options |  |
| enabled | false |
| spark\_application\_info\_options | spark\_application\_info\_options |  |
| enabled | false |
| driver |  |
| sink | false |
| connectorSource | false |
| jvmSource | false |
| stateSource | false |
| executor |  |
| sink | false |
| connectorSource | false |
| jvmSource | false |
| graph | graph |  |
| max\_query\_params | 16 |
| adjacency\_cache\_size\_in\_mb | 128 |
| system\_evaluation\_timeout\_in\_seconds | 180 |
| index\_cache\_size\_in\_mb | 128 |
| analytic\_evaluation\_timeout\_in\_minutes | 10080 |
| schema\_agreement\_timeout\_in\_ms | 10000 |
| realtime\_evaluation\_timeout\_in\_seconds | 30 |
| gremlin\_server |  |
| port | 8182 |
| threadPoolWorker | 2 |
| scriptEngines |  |
| gremlin-groovy |  |
| config |  |
| sandbox\_enabled | false |
| kerberos\_options | kerberos\_options |  |
| keytab | /etc/dse/conf/dse.keytab |
| service\_principal | dse/\_HOST@REALM |
| http\_principal | HTTP/\_HOST@REALM |
| qop | auth |
| user\_level\_latency\_tracking\_options | user\_level\_latency\_tracking\_options |  |
| enabled | false |
| dsefs\_options | dsefs\_options |  |
| work\_dir | /data/dsefs\_dr |
| public\_port | 5598 |
| query\_cache\_size | 2048 |
| compression\_frame\_max\_size | 1048576 |
| gossip\_options |  |
| round\_delay\_ms | 2000 |
| startup\_delay\_ms | 5000 |
| shutdown\_delay\_ms | 10000 |
| service\_startup\_timeout\_ms | 30000 |
| enabled | true |
| rest\_options |  |
| request\_timeout\_ms | 330000 |
| connection\_open\_timeout\_ms | 55000 |
| client\_close\_timeout\_ms | 60000 |
| server\_request\_timeout\_ms | 300000 |
| idle\_connection\_timeout\_ms | 0 |
| private\_port | 5599 |
| keyspace\_name | dsefs\_dr |
| transaction\_options |  |
| transaction\_timeout\_ms | 60000 |
| conflict\_retry\_delay\_ms | 10 |
| conflict\_retry\_count | 40 |
| execution\_retry\_delay\_ms | 1000 |
| execution\_retry\_count | 3 |
| server\_close\_timeout\_ms | 2147483647 |
| data\_directories |  |
| - dir | /data/dsefs/data |
| min\_free\_space | 268435456 |
| storage\_weight | 1 |
| block\_allocator\_options |  |
| overflow\_margin\_mb | 1024 |
| overflow\_factor | 1.05 |
| service\_close\_timeout\_ms | 600000 |
| internode\_authentication |  |
| enabled | true |
| algorithm | HmacSHA256 |
| query\_cache\_expire\_after\_ms | 2000 |
| solr\_request\_handler\_metrics\_options | solr\_request\_handler\_metrics\_options |  |
| enabled | false |
| spark\_daemon\_readiness\_assertion\_interval | spark\_daemon\_readiness\_assertion\_interval | 1000 |
| spark\_shared\_secret\_bit\_length | spark\_shared\_secret\_bit\_length | 256 |
| cql\_solr\_query\_paging | cql\_solr\_query\_paging | off |
| internode\_messaging\_options | internode\_messaging\_options |  |
| client\_max\_connections | 200 |
| port | 8609 |
| performance\_max\_threads | performance\_max\_threads | 32 |
| insights\_options | insights\_options |  |
| log\_dir | /u01/log/dse/insights |
| data\_dir | /data/insights |
| async\_bootstrap\_reindex | async\_bootstrap\_reindex | false |
| alwayson\_sql\_options | alwayson\_sql\_options |  |
| reserve\_port\_wait\_time\_ms | 100 |
| web\_ui\_port | 9077 |
| enabled | true |
| runner\_max\_errors | 10 |
| alwayson\_sql\_status\_check\_wait\_time\_ms | 500 |
| workpool | alwayson\_sql |
| log\_dsefs\_dir | /spark/log/alwayson\_sql |
| auth\_user | alwayson\_sql |
| thrift\_port | 10000 |
| enable\_health\_based\_routing | enable\_health\_based\_routing | true |
| lease\_metrics\_options | lease\_metrics\_options |  |
| enabled | false |
| ram\_buffer\_offheap\_space\_in\_mb | ram\_buffer\_offheap\_space\_in\_mb | 1024 |
| back\_pressure\_threshold\_per\_core | back\_pressure\_threshold\_per\_core | 1024 |
| node\_health\_options | node\_health\_options |  |
| refresh\_rate\_ms | 60000 |
| uptime\_ramp\_up\_period\_seconds | 10800 |
| dropped\_mutation\_window\_minutes | 30 |
| solr\_encryption\_options | solr\_encryption\_options |  |
| decryption\_cache\_offheap\_allocation | true |
| decryption\_cache\_size\_in\_mb | 256 |
| solr\_latency\_snapshot\_options | solr\_latency\_snapshot\_options |  |
| enabled | false |
| db\_summary\_stats\_options | db\_summary\_stats\_options |  |
| enabled | false |
| enable\_index\_disk\_failure\_policy | enable\_index\_disk\_failure\_policy | false |
| resource\_manager\_options | resource\_manager\_options |  |
| worker\_options |  |
| cores\_total | '0.7' |
| memory\_total | '0.6' |
| workpools | [] |
| solr\_cache\_stats\_options | solr\_cache\_stats\_options |  |
| enabled | false |
| cluster\_summary\_stats\_options | cluster\_summary\_stats\_options |  |
| enabled | false |
| max\_memory\_to\_lock\_mb | max\_memory\_to\_lock\_mb | 10240 |
| solr\_slow\_sub\_query\_log\_options | solr\_slow\_sub\_query\_log\_options |  |
| enabled | false |
| system\_key\_directory | system\_key\_directory | /u01/app/dse/conf |
| solr\_index\_stats\_options | solr\_index\_stats\_options |  |
| enabled | false |
| audit\_logging\_options | audit\_logging\_options |  |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| enabled | true |
| included\_keyspaces | ks\_dangky, ks\_danhmuc, ks\_hddt\_system, ks\_hoadon, ks\_hosogoc, ks\_ht\_tacnghiep, ks\_kad, ks\_luutam, ks\_tintuc, ks\_tdt\_system |
|  |  |
| retention\_time | 0 |
| render\_cql\_literals | true |
| cassandra\_audit\_writer\_options |  |
| mode | sync |
| queue\_size | 30000 |
| write\_consistency | QUORUM |
| dropped\_event\_log | /var/log/cassandra/dropped\_audit\_events.log |
| day\_partition\_millis | 3600000 |
| cql\_slow\_log\_options | cql\_slow\_log\_options |  |
| enabled | true |
| threshold | 200 |
| minimum\_samples | 100 |
| ttl\_seconds | 259200 |
| skip\_writing\_to\_db | true |
| num\_slowest\_queries | 5 |
| cql\_solr\_query\_row\_timeout | cql\_solr\_query\_row\_timeout | 10000 |
| solr\_update\_handler\_metrics\_options | solr\_update\_handler\_metrics\_options |  |
| enabled | false |
| ram\_buffer\_heap\_space\_in\_mb | ram\_buffer\_heap\_space\_in\_mb | 1024 |
| cql\_system\_info\_options | cql\_system\_info\_options |  |
| enabled | false |
| advanced\_replication\_options | advanced\_replication\_options |  |
| enabled | false |
| solr\_field\_cache\_enabled | solr\_field\_cache\_enabled | false |
| spark\_ui\_options | spark\_ui\_options |  |
| encryption | inherit |
| encryption\_options |  |
| enabled | false |
| flush\_max\_time\_per\_core | flush\_max\_time\_per\_core | 5 |
| max\_memory\_to\_lock\_fraction | max\_memory\_to\_lock\_fraction | 0.2 |
| performance\_core\_threads | performance\_core\_threads | 4 |
| authorization\_options | authorization\_options |  |
| enabled | true |
| transitional\_mode | disabled |
| allow\_row\_level\_security | false |
| shard\_transport\_options | shard\_transport\_options |  |
|  | user\_memberof\_attribute | memberof |
| ssl\_protocol | TLS |
| group\_search\_type | directory\_search |
| search\_password | redacted |
| all\_parent\_groups\_memberof\_attribute | isMemberOf |
| credentials\_validity\_in\_ms | 0 |
| truststore\_path | '' |
| groups\_update\_interval\_in\_ms | 0 |
| groups\_validity\_in\_ms | 0 |
| search\_validity\_in\_seconds | 0 |
| user\_search\_base | '' |
| user\_search\_filter | (uid={0}) |
| server\_host | '' |
| hostname\_verification | false |
| group\_name\_attribute | cn |
| server\_port | 389 |
| use\_ssl | false |
| truststore\_type | jks |
| connection\_pool |  |
| max\_active | 8 |
| max\_idle | 8 |
| search\_dn | '' |
| extra\_group\_search\_bases | [] |
| group\_search\_filter | (uniquemember={0}) |
| dns\_service\_discovery |  |
| lookup\_timeout\_ms | 5000 |
| retention\_duration\_ms | 600000 |
| polling\_interval\_ms | 0 |
| use\_tls | false |
| extra\_user\_search\_bases | [] |
| ttl\_index\_rebuild\_options | ttl\_index\_rebuild\_options |  |
| fixed\_rate\_period | 300 |
| initial\_delay | 20 |
| max\_docs\_per\_batch | 4096 |
| thread\_pool\_size | 1 |
| load\_max\_time\_per\_core | load\_max\_time\_per\_core | 5 |
| graph\_events | graph\_events |  |
| ttl\_seconds | 600 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

| **THAM SỐ DR\_Ana** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_ANA |  |
| Số lượng Node bổ sung | 16 |  |
| Workload | Analytics + Search |  |

##### Thông số Logical Rack

Logical Rack của DR\_Ana được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 02 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Ana:
* Số lượng node: 16
* Logical rack: 02
* Số lượng nodes trên logical rack dr\_ana1: 8
* Số lượng nodes trên logical rack dr\_ana2: 8
* Thông tin được hiển thị chi tiết theo bảng sau:

| **TT** | **DC** | **Tham số** | **Physical Rack** | | | | **Tổng** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack A11** | **Rack A11** | **Rack D11** | **Rack D11** |
| 1 | DR\_Ana 16 node (RF=2) | Chassis | 1 | 1 | 1 | 1 | 4 |
| Nodes | 4 | 4 | 4 | 4 | 16 |
| Logical Rack ID | dr\_ana1 | dr\_ana1 | dr\_ana2 | dr\_ana2 |  |

##### Thông số các Node CSDL Ana

Thông số cấu hình từng node CSDL ANA như sau:

| **CẤU HÌNH TỪNG NODE ANA** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 \* 1,92TB SSD |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 5.2 TiB |  |
| DNS | 10.64.88.11 |  |
| 10.64.88.12 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Ana

| **STT** | **Keyspace** | **Replicate Factor (DC\_Ana)** | **Replication Strategy** |
| --- | --- | --- | --- |
| 1 | ks\_hoadon | 2 | NetworkTopologyStrategy |
| 3 | ks\_kad | 2 | NetworkTopologyStrategy |
| 5 | ks\_luutam | 2 | NetworkTopologyStrategy |
| 6 | ks\_danhmuc | 2 | NetworkTopologyStrategy |
| 7 | ks\_tdt\_system | 2 | NetworkTopologyStrategy |
| 8 | ks\_hddt\_system | 2 | NetworkTopologyStrategy |
| 9 | ks\_baocao | 2 | NetworkTopologyStrategy |
| 10 | ks\_dangky | 2 | NetworkTopologyStrategy |
| 11 | dse\_leases | 3 | NetworkTopologyStrategy |
| 12 | dse\_security | 3 | NetworkTopologyStrategy |
| 13 | dsefs | 3 | NetworkTopologyStrategy |
| 14 | dse\_audit | 1 | NetworkTopologyStrategy |
| 15 | dse\_analytics | 3 | NetworkTopologyStrategy |
| 16 | dse\_perf | 2 | NetworkTopologyStrategy |
| 17 | system\_auth | 3 | NetworkTopologyStrategy |
| 18 | system\_distributed | 2 | NetworkTopologyStrategy |
| 19 | spark\_jobserver | 2 | NetworkTopologyStrategy |
| 20 | HiveMetaStore | 3 | NetworkTopologyStrategy |
| 21 | OpsCenter | 2 | NetworkTopologyStrategy |
| 22 | monitor | 2 | NetworkTopologyStrategy |
| 23 | temp | 2 | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Ana, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Ana được phân bố theo bảng sau:

| **Keyspace** | **DR\_Ana** | **Keyspace replication Strategy** |
| --- | --- | --- |
| **ks\_hoadon** | 2 | NetworkTopologyStrategy |
| **ks\_danhmuc** | 2 | NetworkTopologyStrategy |
| **ks\_dangky** | 2 | NetworkTopologyStrategy |
| **ks\_hddt\_system** | 2 | NetworkTopologyStrategy |
| **ks\_luutam** | 2 | NetworkTopologyStrategy |
| **ks\_tdt\_system** | 2 | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL ANA tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 10 phút kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Mỗi máy chủ được cấu hình log với dung lượng không quá 500Mb hoặc thời gian lưu trữ không quá 6 tháng.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.158 | 9997 |
| 10.64.212.159 | 9997 |
| 10.64.212.213 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.215 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |

## Thiết kế hệ thống máy chủ CSDL MTT bổ sung tại TTDL dự phòng

### Mô hình triển khai Cơ sở dữ liệu

Tại trung tâm dữ liệu dự phòng, các máy chủ cơ sở dữ liệu được cài đặt và cấu hình thành 01 Cluster Database: Cluster MTT

Các cluster này cũng được quản trị, giám sát bằng các máy chủ quản trị OpsCenter chạy HA, quản trị chung cả hệ thống CSLD tại trung tâm dữ liệu chính và dự phòng. Trên các cluster tạo ra các DC phục vụ các workload khác nhau bao gồm: DR\_Trans, DR\_Search, DR\_Docs và DR\_Ana.

Hệ thống máy chủ CSDL của ứng dụng hóa đơn điện tử được bổ sung tạm thời (phục vụ chuyển đổi DC sang DC mới) các máy chủ lấy từ hợp đồng số 34/2024/HĐKT/TCT-TECAPRO-OSP-NGS-FPT IS bao gồm 12 máy chủ Dell bổ sung cho các cụm cluster như sau:

* Máy chủ CSDL Transaction: gồm 4 thiết bị Dell PowerEdge C6620
* Máy chủ CSDL Search: gồm 4 thiết bị Dell PowerEdge C6620
* Máy chủ CSDL XML: gồm 4 thiết bị Dell PowerEdge C6620
* Máy chủ CSDL Ana: gồm 4 thiết bị Dell PowerEdge C6620

Trong dự án số lượng máy chủ cơ sở dữ liệu được bổ sung như sau:

| **Tên DC** | **DR\_Trans** | **DR\_Search** | **DR\_Docs** | **DC\_Ana** |
| --- | --- | --- | --- | --- |
| Số lượng Node hiện tại | 6 | 4 | 8 | 4 |
| Số lượng Node bổ sung | 4 | 4 | 4 | 4 |
| Số lượng Node sau mở rộng | 10 | 8 | 12 | 8 |
| Workload | Cassandra | Search | Cassandra | Analytics + Search |

#### Mô hình tổng quan hệ thống CSDL

Dự án phục vụ mục đích mở rộng cluster MTT nên không làm thay đổi mô hình tổng quan của hệ thống CSDL. Hệ thống vẫn bao gồm Cluster MTT và Cluster MGMT.

Diagram, timeline

Description automatically generated

Hình 10: Mô hình tổng quan hệ thống CSDL

#### Mô hình thiết kế tại TTDL dự phòng

A diagram of a cluster

AI-generated content may be incorrect.

Sau khi bổ sung node, cluster MTT tại DR site sẽ bao gồm:

* 10 Node trong DR\_Trans
* 8 Node trong DR\_Search
* 12 Node trong DR\_Docs
* 8 Node trong DR\_Ana

#### Hệ thống quản trị tập trung

##### Hệ thống quản lý máy chủ vật lý

Phần cứng máy chủ được quản lý tập trung bởi giải pháp Oneview của HPE. Thông tin của máy chủ Oneview:

| **STT** | **Hostname** | **IP** | **Giao thức** | **Username** | **Password** |
| --- | --- | --- | --- | --- | --- |
|  | drm-hpeoneview | 10.64.167.238 | TCP/UDP | Administrator | \*\*\*\*\*\*\*\* |

Các cổng kết nối cần mở:

| **STT** | **Địa chỉ nguồn** | **Description** | **Địa chỉ đích** | **Description** | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 10.64.170.223-10.64.170.238 | Server ILOs | 10.64.167.238 | Oneview | 123:UDP | 1 | HPE OneView acts as an NTP server, iLO requires access. | Vĩnh viễn |
| 2 | 10.64.167.238 | Oneview | 10.64.170.223-10.64.170.238 | Server ILOs | 161:UDP | 1 | Supports SNMP GET calls to monitored and managed devices, such as, server iLO, HPE Intelligent Power Distribution Unit, and SAN Managers. | Vĩnh viễn |
| 3 | 10.64.167.238 | Oneview | 10.64.170.223-10.64.170.238 | Server ILOs | 443 | 2 | Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. | Vĩnh viễn |
| 4 | 10.64.211.11  10.64.211.14 | Management Workstation | 10.64.170.223-10.64.170.238 | Server ILOs | 443 | 1 | Used for secure SSL access to the iLO, Frame link module, remote support access to Hewlett Packard Enterprise, and other devices. | Vĩnh viễn |

### Thiết kế chi tiết hệ thống máy chủ Search

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL Search gồm 8 node được cài đặt trên các khung máy chủ HPE Apollo n2600 Gen10 Plus. Một Chassis HPE Apollo n2600 Gen10 Plus 2U được lắp đặt tối đa 04 máy chủ HPE ProLiant XL220n Gen10 Plus. Mỗi HPE ProLiant XL220n Gen10 Plus có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data.

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 switch chuyển mạch dữ liệu khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| **Site** | **Trung tâm dữ liệu dự phòng** |
| --- | --- |
| Tên DC​ | DR\_Search​ |
| Số lượng Node bổ sung tại DC​ | 4 |
| Workload​ | Search ​ |

##### Bảng phân bổ lắp đặt Rack

Các máy chủ CSDL Search được phân bổ trên 01 Rack vật lý như sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **U** | **Rack D11** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| U12-U13 | dri-ehdsearchc6600ch15 | 1900 | 1520 | 2 | 4772.8 | 43 |

Bảng lắp đặt các máy chủ CSDL Search trên Rack chi tiết như sau:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| 1 | D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 |
| 2 | dri-ehdmttsearchdb206 |
| 3 | dri-ehdmttsearchdb207 |
| 4 | dri-ehdmttsearchdb208 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A list of numbers and letters

Description automatically generated

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A diagram of a computer server

Description automatically generated

Hình 12: Kết nối quản trị máy chủ Search

Thông tin IP quản trị của máy chủ CSDL Search được thể hiện chị tiết qua bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP iDRAC** | **Netmask** | **GateWay** |
| 1 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 | 309 | 10.64.170.235 | 255.255.255.0 | 10.64.170.1 |
| 2 |  | dri-ehdmttsearchdb206 | 309 | 10.64.170.236 | 255.255.255.0 | 10.64.170.1 |
| 3 |  | dri-ehdmttsearchdb207 | 309 | 10.64.170.237 | 255.255.255.0 | 10.64.170.1 |
| 4 |  | dri-ehdmttsearchdb208 | 309 | 10.64.170.238 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL Search được thể hiện ở bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP Data** | **Netmask** | **GateWay** |
| 1 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 | 233 | 10.64.159.205 | 255.255.255.0 | 10.64.159.1 |
| 2 |  | dri-ehdmttsearchdb206 | 233 | 10.64.159.206 | 255.255.255.0 | 10.64.159.1 |
| 3 |  | dri-ehdmttsearchdb207 | 233 | 10.64.159.207 | 255.255.255.0 | 10.64.159.1 |
| 4 |  | dri-ehdmttsearchdb208 | 233 | 10.64.159.208 | 255.255.255.0 | 10.64.159.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL Search có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng như sau:

A diagram of a computer server

Description automatically generated

Hình 13: Mô hình kết nối máy chủ CSDL Search

Thông tin kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | | | | | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |  |  |  |  | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/43 | Access | 309 | MGMT | Đồng - 1Gb | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/27 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb205 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb206 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/44 | Access | 309 | MGMT | Đồng - 1Gb | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb206 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/28 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb206 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb207 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/45 | Access | 309 | MGMT | Đồng - 1Gb | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb207 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/29 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb207 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb208 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/46 | Access | 309 | MGMT | Đồng - 1Gb | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb208 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/30 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |
| D11 | U5-U6 | dri-ehdsearchc6600ch15 | dri-ehdmttsearchdb208 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G | |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Search

Bảng thông số các máy chủ CSDL Search như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (GB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdmttsearchdb205 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.159.205 |
| 2 | dri-ehdmttsearchdb206 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.159.206 |
| 3 | dri-ehdmttsearchdb207 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.159.207 |
| 4 | dri-ehdmttsearchdb208 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.159.208 |

Thông số cấu hình các dịch vụ mạng

|  |  |
| --- | --- |
| DNS Server | 10.64.88.11, 10.64.88.12 |
| NTP Server | 10.64.68.26 |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ debug, khác của OS | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:
* Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.
* HĐH của máy chủ sẽ được ưu tiên về tốc độ xử lý. Do đó HĐH sẽ được cài đặt lưu trên RAID0 Array tạo từ 01 ổ cứng.
* Với phân vùng solr\_index, trên HĐH sẽ cài đặt để lưu trên 01 ổ cứng Non-RAID.
* Với phân vùng data, dữ liệu sẽ được lưu trên các ổ cứng không tạo RAID. Trên HĐH sẽ sử dụng LVM để gộp thành 02 ổ cứng Non-RAID này thành 1 ổ logic.
* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 960 GB (RAID 0) | sda | sda1 | 600 MiB | - | - | /boot/efi | efi |  |
| sda2 | 1 GiB | - | - | /boot | xfs |  |
| sda3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sda4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sda6 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 664 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 960 GB (No Raid) | sdb | sdb1 | 650 GiB | vg\_solr | lv\_solr | /solr\_index | xfs |  |
| Free | 224 GiB |  |  |  |  | dự phòng |
| 3 | 01 x 960 GB (No Raid) | sdc | sdc1 | 1.746 TiB | vg\_data | lv\_data | /data | xfs |  |
| 4 | 01 x 960 GB (No Raid) | sdd | sdd1 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

|  |  |
| --- | --- |
| **Thông số** | **Value** |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các tham số khác:

|  |  |  |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| Disable CPU frequency scaling | *for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done* | Disable CPU frequency scaling |
| *zone\_reclaim\_mode* | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | *sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab*  *sudo swapoff –all* | Disable swap |
| Optimize SSDs |  |  |
| */sys/block/device\_name/queue/schedu* | *deadline* | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| */sys/block/device\_name/queue/nr\_requests* | *128* | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| */sys/class/block/device\_name/queue/rotational* | *0* |  |
| */sys/class/block/device\_name/queue/read\_ahead\_kb* | *8* |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Thông số User và CSDL

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| mtt\_adhoc | mtt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng HDDT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| mtt\_app | mtt\_app | ks\_mtt\_system.mtt\_service\_config | SELECT |
| mtt\_category | mtt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_mtt\_system ks\_dangky | SELECT, UPDATE |
| hddt\_config | hddt\_config | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_delegation | hddt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_examination | hddt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| hddt\_explanation | hddt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| hddt\_explanation\_tvan | hddt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice | hddt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| hddt\_invoice\_code | hddt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| hddt\_invoice\_code\_adhoc | hddt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| hddt\_job | hddt\_job | ks\_hddt\_system | SELECT |
| hddt\_job\_config | hddt\_job\_config | ks\_hddt\_system ks\_danhmuc | SELECT, UPDATE |
| hddt\_message | hddt\_message | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| hddt\_query | hddt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration | hddt\_registration | ks\_hddt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| hddt\_registration\_status | hddt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| hddt\_security\_official | hddt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_security\_taxpayer | hddt\_security\_taxpayer | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_sync | hddt\_sync | ks\_danhmuc | SELECT, UPDATE |
| hddt\_system | hddt\_system | ks\_hddt\_system | SELECT, UPDATE |
| hddt\_tax\_risk | hddt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_expired | hddt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tin\_status | hddt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_tvan\_status | hddt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| hddt\_verification | hddt\_verification | ks\_hddt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_hddt\_to\_dwh\_ods | job\_hddt\_to\_dwh\_ods | ks\_dangky.hddt\_dky  ks\_dangky.hddt\_tkhai  ks\_hoadon.hddt\_bthctiet\_mgr  ks\_hoadon.hddt\_bthop  ks\_hoadon.hddt\_hdhhdvu  ks\_hoadon.hddt\_hdon  ks\_hoadon.hddt\_tbhgthdon  ks\_hoadon.hddt\_tbssdt  ks\_hosogoc.hddt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_hddt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_hddt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
| 2 | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 8443,8888,61620:TCP | 1 | Mở cổng từ các DSE node đến máy chủ quản trị DSE OpsCenter | Vĩnh viễn |
| 3 | 10.64.211.14, 10.64.211.12, 10.64.211.11 | Máy chủ Terminal | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 22,4040,5598,5599,7080,7081,8983,9042,9142,9091,9077,9999,18080:TCP | 1 | Mở cổng từ Remote client tới các DSE node | Vĩnh viễn |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 (3 IP) | Dashboard Grafana | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 10.64.212.206 => 10.64.212.208 (3 IP) | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP)  10.64.98.112 🡪 10.64.98.121 | HDDT Core Microservice | 10.64.159.205=> 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Search mới | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.159.205 🡪 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Search mới | Vĩnh viễn |
| 3 | 10.64.90.153 🡪 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.159.205 🡪 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Search mới | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.159.205 🡪 10.64.159.208 | Máy chủ DSE Search mới (MTT DR\_Search) | 10.64.100.207 => 10.64.100.212,  10.64.159.201 => 10.64.159.202, | DSE (MTT DC\_Search, DR\_Search) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ Search cũ sang các máy chủ Search mới | Vĩnh viễn |

#### Thông số chi tiết CSDL Search

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Loại** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| Security | client\_encryption\_options | enabled TRUE |
| General | num\_tokens | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | 2 |
| tpc\_pending\_requests\_limit | 256 |
| Directory | data\_file\_directories | /data/data |
| commitlog\_directory | /commitlog |
| saved\_caches\_directory | /data/saved\_caches |
| Ports | native\_transport\_port\_ssl | 9142 |
| NodeSync | rate\_in\_kb | 10240 |
| Caches | row\_cache\_size\_in\_mb | 500 |
| row\_cache\_save\_period | 36000 |
| Timeouts | read\_request\_timeout\_in\_ms | 5000 |
| write\_request\_timeout\_in\_ms | 2000 |
| Snapshots | incremental\_backups | TRUE |
| auto\_snapshot | TRUE |
| Hinted Handoff | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hints\_delivery\_threads | 6 |
| hints\_directory | /data/hints |
| Change Data Capture | cdc\_raw\_directory | /data/cdc\_raw |
| Miscellaneous | metadata\_directory | /data/metadata |

* Thông số File dse.yaml:

| **Loại** | **Tham số** | **Tham số thành phần** | **Giá trị** |
| --- | --- | --- | --- |
| DSE Authorizer Options | authorization\_options | enabled | TRUE |
| transitional\_mode | disabled |
| allow\_row\_level\_security | FALSE |
| DSE Metrics Collector | insights\_options | data\_dir | /data/insights |
| log\_dir | /u01/log/dse/insights |
| Encryption Settings | system\_key\_directory |  | /u01/app/dse/conf |
| Audit Logging Settings | audit\_logging\_options | enabled | TRUE |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| Miscellaneous | internode\_messaging\_options | client\_max\_connections | 200 |
| port | 8609 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

|  |  |  |
| --- | --- | --- |
| **THAM SỐ DR\_SEARCH** | | |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_Search |  |
| Số lượng Node bổ sung | 4 |  |
| Workload | Search |  |

##### Thông số Logical Rack

Logical Rack của DR\_Search được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 01 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Search:
* Số lượng node: 4
* Logical rack: 2
* Số lượng nodes trên logical rack dr\_search1: 2
* Số lượng nodes trên logical rack dr\_search2: 2
* Thông tin được hiển thị chi tiết theo bảng sau:

| **TT** | **DC** | **Tham số** | **Physical Rack** | | **Tổng** |
| --- | --- | --- | --- | --- | --- |
| **Rack D11** | |
| 1 | DR\_Search 4 node (RF=2) | Chassis | 1 | | 1 |
| Nodes | 4 | | 4 |
| Logical Rack ID | dr\_search1 | dr\_search2 |  |

##### Thông số các Node CSDL Search

Thông số cấu hình từng node CSDL Search như sau:

| **CẤU HÌNH TỪNG NODE SEARCH** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 x 960GB (SSD) |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 1.7TiB |  |
| DNS | 10.64.89.11 |  |
| 10.64.89.13 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Search

Danh sách các keyspace cho DR\_Search: Triển khai CSDL NoSQL Datastax Enterprise (DSE) cho các nhu cầu xử lý giao dịch trực tuyến.

Bao gồm các Keyspace:

| **Tên keyspace** | **Chú thích** | **Keyspace replication Strategy** |
| --- | --- | --- |
| ks\_danhmuc (Danh mục) | Phân vùng lưu trữ thông tin danh mục của hệ thống HĐĐT. Danh mục đồng bộ từ các hệ thống khác của TCT như: Cơ quan thế, địa bành hành chính, phòng ban… Danh mục riêng của hệ thống HĐĐT như Loại tờ khai, mẫu đăng ký, mẫu thông báo… | NetworkTopologyStrategy |
| ks\_dangky (Đăng ký) | Phân vùng lưu thông tin liên quan đến đăng ký sử dụng HĐĐT của NNT, TVAN, DNKNTT. | NetworkTopologyStrategy |
| ks\_hoadon (Hóa đơn) | Phân vùng lưu trữ thông tin các bảng liên quan đến nghiệp vụ chính: Tiếp nhận, xử lý thông tin HĐĐT có mã, không mã, thông báo hủy giải trình và hóa đơn trong giai đoạn chuyển tiếp. | NetworkTopologyStrategy |
| ks\_luutam  (Lưu tạm) | Lưu trữ tạm thời các thông tin hồ sơ... | NetworkTopologyStrategy |
| ks\_hddt\_system | Phân quyền, cấu hình, user của ứng dụng | NetworkTopologyStrategy |
| ks\_tdt\_system | Phân quyền, cấu hình, user của ứng dụng tem điện tử | NetworkTopologyStrategy |
| OpsCenter | Quản trị OpsCenter | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Search, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Search được phân bố theo bảng sau:

| **Keyspace** | **DR\_Search** | **Keyspace replication Strategy** |
| --- | --- | --- |
| **ks\_hoadon** | 2 | NetworkTopologyStrategy |
| **ks\_danhmuc** | 2 | NetworkTopologyStrategy |
| **ks\_dangky** | 2 | NetworkTopologyStrategy |
| **ks\_hddt\_system** | 2 | NetworkTopologyStrategy |
| **ks\_luutam** | 2 | NetworkTopologyStrategy |
| **ks\_tdt\_system** | 2 | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL Search tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 5 phút (300 giây) kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Không giới hạn kích thước và lưu trữ không quá 4 tuần.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.168.106 | 9997 |
| 10.64.168.107 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.168.19 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |

### Thiết kế chi tiết hệ thống máy chủ Transaction

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL Transaction gồm 10 node được cài đặt trên các khung máy chủ HPE Apollo n2600 Gen10 Plus. Một Chassis HPE Apollo n2600 Gen10 Plus 2U được lắp đặt tối đa 04 máy chủ HPE ProLiant XL220n Gen10 Plus. Mỗi HPE ProLiant XL220n Gen10 Plus có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data.

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 switch chuyển mạch dữ liệu khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| **Site** | Trung tâm dữ liệu dự phòng |
| --- | --- |
| **Tên DC​** | DR\_Trans​ |
| **Số lượng Node bổ sung tại DC​** | 4 |
| **Workload​** | Cassandra​ |

##### Bảng phân bổ lắp đặt Rack

* Các máy chủ CSDL Transaction được phân bổ trên 01 Rack vật lý như sau:

| **Rack** | **U** | **Chasiss** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| --- | --- | --- | --- | --- | --- | --- | --- |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | 1900 | 1520 | 2 | 4772.8 | 43 |

* Bảng lắp đặt các máy chủ CSDL Transaction trên Rack chi tiết như sau:

| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| --- | --- | --- | --- | --- |
| 1 | D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 |
| 2 | dri-ehdmtttransdb208 |
| 3 | dri-ehdmtttransdb209 |
| 4 | dri-ehdmtttransdb210 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A list of numbers and letters

Description automatically generated

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A diagram of a computer server

Description automatically generated

Hình 14: Kết nối quản trị máy chủ Trans

Thông tin IP quản trị của máy chủ CSDL Transaction được thể hiện chị tiết qua bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP iDRAC** | **Netmask** | **GateWay** |
| 1 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 | 309 | 10.64.170.227 | 255.255.255.0 | 10.64.170.1 |
| 2 |  | dri-ehdmtttransdb208 | 309 | 10.64.170.228 | 255.255.255.0 | 10.64.170.1 |
| 3 |  | dri-ehdmtttransdb209 | 309 | 10.64.170.229 | 255.255.255.0 | 10.64.170.1 |
| 4 |  | dri-ehdmtttransdb210 | 309 | 10.64.170.230 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL Transaction được thể hiện ở bảng sau:

| **No.** | **Chassis** | **Device** | **VLAN** | **IP Data** | **Netmask** | **GateWay** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 | 232 | 10.64.158.207 | 255.255.255.0 | 10.64.158.1 |
| 2 |  | dri-ehdmtttransdb208 | 232 | 10.64.158.208 | 255.255.255.0 | 10.64.158.1 |
| 3 |  | dri-ehdmtttransdb209 | 232 | 10.64.158.209 | 255.255.255.0 | 10.64.158.1 |
| 4 |  | dri-ehdmtttransdb210 | 232 | 10.64.158.210 | 255.255.255.0 | 10.64.158.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL Trans có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng máy như sau:

A diagram of a computer server

Description automatically generated

*Mô hình kết nối máy chủ CSDL Trans*

Thông tin kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | |  |  |  | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |  |  |  |  |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/30 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/19 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb207 | P2 | Active |  |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb208 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/31 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb208 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/20 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb208 | P2 | Active |  |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb209 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/32 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb209 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/21 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb209 | P2 | Active |  |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb210 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/33 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb210 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/22 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U10-U11 | dri-ehdtransc6600ch15 | dri-ehdmtttransdb210 | P2 | Active |  |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Transaction

Bảng thông số các máy chủ CSDL Transaction như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (GB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdmtttransdb207 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.158.207 |
| 2 | dri-ehdmtttransdb208 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.158.208 |
| 3 | dri-ehdmtttransdb209 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.158.209 |
| 4 | dri-ehdmtttransdb210 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.158.210 |

Thông số cấu hình các dịch vụ mạng

|  |  |
| --- | --- |
| DNS Server | 10.64.88.11, 10.64.88.12 |
| NTP Server | 10.64.68.26 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

|  |  |
| --- | --- |
| **Thông số** | **Value** |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các tham số khác:

| **Tham số** | **Giá trị** | **Chú thích** |
| --- | --- | --- |
| Disable CPU frequency scaling | *for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done* | Disable CPU frequency scaling |
| *zone\_reclaim\_mode* | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | *sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab*  *sudo swapoff –all* | Disable swap |
| Optimize SSDs |  |  |
| */sys/block/device\_name/queue/schedu* | *deadline* | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| */sys/block/device\_name/queue/nr\_requests* | *128* | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| */sys/class/block/device\_name/queue/rotational* | *0* |  |
| */sys/class/block/device\_name/queue/read\_ahead\_kb* | *8* |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ debug, khác của OS | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:
* Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.
* HĐH của máy chủ sẽ được ưu tiên về tốc độ xử lý. Do đó HĐH sẽ được cài đặt lưu trên RAID0 Array tạo từ 01 ổ cứng.
* Với phân vùng data, dữ liệu sẽ được lưu trên các ổ cứng không tạo RAID. Trên HĐH sẽ sử dụng LVM để gộp thành 03 ổ cứng Non-RAID này thành 1 ổ logic.
* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 960 GB (RAID 0) | sda | sda1 | 600 MiB | - | - | /boot/efi | efi |  |
| sda2 | 1 GiB | - | - | /boot | xfs |  |
| sda3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sda4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sda5 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 664 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 960 GB (No Raid) | sdb | sdb1 | 2.619 TiB | vg\_data | lv\_data | /data | xfs |  |
| 3 | 01 x 960 GB (No Raid) | sdc | sdc1 |
| 4 | 01 x 960 GB (No Raid) | sdd | sdd1 |

##### Thông số User và CSDL

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| mtt\_adhoc | mtt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng MTT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| mtt\_app | mtt\_app | ks\_mtt\_system.mtt\_service\_config | SELECT |
| mtt\_category | mtt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_mtt\_system ks\_dangky | SELECT, UPDATE |
| mtt\_config | mtt\_config | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_delegation | mtt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_examination | mtt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| mtt\_explanation | mtt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| mtt\_explanation\_tvan | mtt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice | mtt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice\_code | mtt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| mtt\_invoice\_code\_adhoc | mtt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| mtt\_job | mtt\_job | ks\_mtt\_system | SELECT |
| mtt\_job\_config | mtt\_job\_config | ks\_mtt\_system ks\_danhmuc | SELECT, UPDATE |
| mtt\_message | mtt\_message | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_query | mtt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration | mtt\_registration | ks\_mtt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration\_status | mtt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| mtt\_security\_official | mtt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_security\_taxpayer | mtt\_security\_taxpayer | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_sync | mtt\_sync | ks\_danhmuc | SELECT, UPDATE |
| mtt\_system | mtt\_system | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_tax\_risk | mtt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_expired | mtt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_status | mtt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tvan\_status | mtt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_verification | mtt\_verification | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_mtt\_to\_dwh\_ods | job\_mtt\_to\_dwh\_ods | ks\_dangky.mtt\_dky  ks\_dangky.mtt\_tkhai  ks\_hoadon.mtt\_bthctiet\_mgr  ks\_hoadon.mtt\_bthop  ks\_hoadon.mtt\_hdhhdvu  ks\_hoadon.mtt\_hdon  ks\_hoadon.mtt\_tbhgthdon  ks\_hoadon.mtt\_tbssdt  ks\_hosogoc.mtt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_mtt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
|  |  |  |  |  |  |  |  |  |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 (3 IP) | Dashboard Grafana | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 10.64.212.206 => 10.64.212.208 (3 IP) | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP),  10.64.98.112 -> 10.64.98.121 | HDDT Core Microservice | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Trans mới | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Trans mới | Vĩnh viễn |
| 3 | 10.64.90.153 => 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Trans mới | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.158.207=> 10.64.158.210 | Máy chủ DSE Transaction mới (MTT DR\_Trans) | 10.64.99.201 => 10.64.99.208,  10.64.158.201 => 10.64.99.206 | DSE (MTT DC\_Trans, DR\_Trans) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ Transaction cũ sang các máy chủ Transaction mới | Vĩnh viễn |

#### Thông số chi tiết CSDL Trans

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Loại** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| Security | client\_encryption\_options | enabled TRUE |
| General | num\_tokens | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | 3 |
| tpc\_pending\_requests\_limit | 256 |
| tpc\_cores |  |
| Directory | data\_file\_directories | /data/data |
| commitlog\_directory | /commitlog |
| saved\_caches\_directory | /data/saved\_caches |
| Ports | native\_transport\_port\_ssl | 9142 |
| NodeSync | rate\_in\_kb | 10240 |
| Caches | row\_cache\_size\_in\_mb | 500 |
| row\_cache\_save\_period | 36000 |
| Timeouts | read\_request\_timeout\_in\_ms | 5000 |
| write\_request\_timeout\_in\_ms | 2000 |
| stream\_outbound\_permits\_in\_mb | 8 |
| input\_stream\_channel\_timeout\_in\_ms | 432000000 |
| Snapshots | incremental\_backups | TRUE |
| auto\_snapshot | TRUE |
| Hinted Handoff | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hints\_delivery\_threads | 6 |
| hints\_directory | /data/hints |
| Change Data Capture | cdc\_raw\_directory | /data/cdc\_raw |
| Miscellaneous | metadata\_directory | /data/metadata |
| Cluster Communication | endpoint\_snitch | GossipingPropertyFileSnitch |
| zerocopy\_streaming\_enabled | FALSE |

* Thông số File dse.yaml:

| **Loại** | **Tham số** | **Tham số thành phần** | **Giá trị** |
| --- | --- | --- | --- |
| DSE Authorizer Options | authorization\_options | enabled | TRUE |
| transitional\_mode | disabled |
| allow\_row\_level\_security | FALSE |
| DSE Metrics Collector | insights\_options | data\_dir | /data/insights |
| log\_dir | /u01/log/dse/insights |
| Encryption Settings | system\_key\_directory |  | /u01/app/dse/conf |
| Audit Logging Settings | audit\_logging\_options | enabled | TRUE |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| Miscellaneous | internode\_messaging\_options | client\_max\_connections | 200 |
| port | 8609 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

|  |  |  |
| --- | --- | --- |
| **THAM SỐ DR\_TRANS** | | |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_Trans |  |
| Số lượng Node bổ sung | 4 |  |
| Workload | Cassandra |  |

##### Thông số Logical Rack

Logical Rack của DR\_Trans được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 01 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Trans:
* Số lượng node: 4
* Logical rack: 02
* Số lượng nodes trên logical rack dr-trans1: 2
* Số lượng nodes trên logical rack dr-trans2: 2
* Thông tin được hiển thị chi tiết theo bảng sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TT** | **DC** | **Tham số** | **Physical Rack** | | **Tổng** |
| **Rack D11** | |
| 1 | DR\_Trans 4 node (RF=2) | Chassis | 1 | | 1 |
| Nodes | 4 | | 4 |
| Logical Rack ID | dr\_trans1 | dr\_trans2 |  |

##### Thông số các Node CSDL Transaction

Thông số cấu hình từng node CSDL Transaction như sau:

| **CẤU HÌNH TỪNG NODE TRANS** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 x 960GB (SSD) |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 2.6TiB |  |
| DNS | 10.64.88.11 |  |
| 10.64.88.12 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Trans

Danh sách các keyspace cho DR\_Trans: Triển khai CSDL NoSQL Datastax Enterprise (DSE) cho các nhu cầu xử lý giao dịch trực tuyến.

Bao gồm các Keyspace:

| **Tên keyspace** | **Chú thích** | **Keyspace replication Strategy** |
| --- | --- | --- |
| ks\_danhmuc (Danh mục) | Phân vùng lưu trữ thông tin danh mục của hệ thống HĐĐT. Danh mục đồng bộ từ các hệ thống khác của TCT như: Cơ quan thế, địa bành hành chính, phòng ban… Danh mục riêng của hệ thống HĐĐT như Loại tờ khai, mẫu đăng ký, mẫu thông báo… | NetworkTopologyStrategy |
| ks\_dangky (Đăng ký) | Phân vùng lưu thông tin liên quan đến đăng ký sử dụng HĐĐT của NNT, TVAN, DNKNTT. | NetworkTopologyStrategy |
| ks\_hoadon (Hóa đơn) | Phân vùng lưu trữ thông tin các bảng liên quan đến nghiệp vụ chính: Tiếp nhận, xử lý thông tin HĐĐT có mã, không mã, thông báo hủy giải trình và hóa đơn trong giai đoạn chuyển tiếp. | NetworkTopologyStrategy |
| ks\_luutam  (Lưu tạm) | Lưu trữ tạm thời các thông tin hồ sơ... | NetworkTopologyStrategy |
| ks\_hddt\_system | Phân quyền, cấu hình, user của ứng dụng | NetworkTopologyStrategy |
| ks\_tdt\_system | Phân quyền, cấu hình, user của ứng dụng tem điện tử | NetworkTopologyStrategy |
| OpsCenter | Quản trị OpsCenter | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Trans, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Trans được phân bố theo bảng sau:

| **Keyspace** | **DR\_Trans** | **Keyspace replication Strategy** |
| --- | --- | --- |
| **ks\_hoadon** | 2 | NetworkTopologyStrategy |
| **ks\_danhmuc** | 2 | NetworkTopologyStrategy |
| **ks\_dangky** | 2 | NetworkTopologyStrategy |
| **ks\_hddt\_system** | 2 | NetworkTopologyStrategy |
| **ks\_luutam** | 2 | NetworkTopologyStrategy |
| **ks\_tdt\_system** | 2 | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL Trans tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 10 phút kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Mỗi máy chủ được cấu hình log với dung lượng không quá 500Mb hoặc thời gian lưu trữ không quá 6 tháng.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.158 | 9997 |
| 10.64.212.159 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.215 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |

### Thiết kế chi tiết hệ thống máy chủ Docs

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL Docs được bổ sung tạm thời 8 node (phục vụ chuyển đổi DC sang DC mới) được cài đặt trên các máy chủ mật độ cao Dell PowerEdge C6620. Một Chassis Dell PowerEdge C6600 2U được lắp đặt 04 máy chủ Dell PowerEdge C6620. Mỗi máy chủ Dell PowerEdge C6620 có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data..

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 switch chuyển mạch dữ liệu khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| **Site** | Trung tâm dữ liệu dự phòng |
| --- | --- |
| **Tên DC​** | DR\_Docs |
| **Số lượng Node bổ sung tại DC​** | 4 |
| **Workload​** | Cassandra​​ |

##### Bảng phân bổ lắp đặt Rack

* Các máy chủ CSDL XML được phân bổ trên 01 Rack vật lý như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chasiss** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| D11 | U7- U8 | dri-ehdxmlc6600ch17 | 1900 | 1520 | 2 | 4772.8 | 43 |

* Bảng lắp đặt các máy chủ CSDL XML trên Rack chi tiết như sau:

| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| --- | --- | --- | --- | --- |
| 1 | D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 |
| 2 | dri-ehdmttxmldb210 |
| 3 | dri-ehdmttxmldb211 |
| 4 | dri-ehdmttxmldb212 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A list of numbers and letters

Description automatically generated

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A diagram of a computer server

Description automatically generated

Hình 15: Kết nối quản trị máy chủ XML

Thông tin IP quản trị của máy chủ CSDL XML được thể hiện chị tiết qua bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP iDRAC** | **Netmask** | **GateWay** |
| 1 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 | 309 | 10.64.170.231 | 255.255.255.0 | 10.64.170.1 |
| 2 |  | dri-ehdmttxmldb210 | 309 | 10.64.170.232 | 255.255.255.0 | 10.64.170.1 |
| 3 |  | dri-ehdmttxmldb211 | 309 | 10.64.170.233 | 255.255.255.0 | 10.64.170.1 |
| 4 |  | dri-ehdmttxmldb212 | 309 | 10.64.170.234 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL XML được thể hiện ở bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP Data** | **Netmask** | **GateWay** |
| 1 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 | 235 | 10.64.161.209 | 255.255.255.0 | 10.64.161.1 |
| 2 |  | dri-ehdmttxmldb210 | 235 | 10.64.161.210 | 255.255.255.0 | 10.64.161.1 |
| 3 |  | dri-ehdmttxmldb211 | 235 | 10.64.161.211 | 255.255.255.0 | 10.64.161.1 |
| 4 |  | dri-ehdmttxmldb212 | 235 | 10.64.161.212 | 255.255.255.0 | 10.64.161.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL XML có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng máy như sau:

A diagram of a computer hardware

Description automatically generated

*Mô hình kết nối máy chủ CSDL XML*

Thông tin chi tiết kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | |  |  |  | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |  |  |  |  |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/39 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/23 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb209 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb210 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/40 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb210 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/24 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb210 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb211 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/41 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb211 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/25 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb211 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb212 | iDRAC |  |  | A01 | U10 | DR-MGMT-ACCSW03 | ge-0/0/42 | Access | 309 | MGMT | Đồng - 1Gb |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb212 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/26 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| D11 | U7-U8 | dri-ehdxmlc6600ch17 | dri-ehdmttxmldb212 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Docs

Bảng thông số các máy chủ CSDL Docs như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (GB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdmttxmldb209 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.161.209 |
| 2 | dri-ehdmttxmldb210 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.161.210 |
| 3 | dri-ehdmttxmldb211 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.161.211 |
| 4 | dri-ehdmttxmldb212 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.161.212 |

Thông số cấu hình các dịch vụ mạng

|  |  |
| --- | --- |
| DNS Server | 10.64.88.11, 10.64.88.12 |
| NTP Server | 10.64.68.26 |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ monitor, debug, khác | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:

+ Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.

+ HĐH của máy chủ sẽ được ưu tiên về tốc độ xử lý. Do đó HĐH sẽ được cài đặt lưu trên RAID0 Array tạo từ 01 ổ cứng.

+ Với phân vùng data, dữ liệu sẽ được lưu trên các ổ cứng không tạo RAID. Trên HĐH sẽ sử dụng LVM để gộp thành 03 ổ cứng Non-RAID này thành 1 ổ logic.

* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 1.92 TB (RAID 0) | sda | sdd1 | 600 MiB | - | - | /boot/efi | efi |  |
| sdd2 | 1 GiB | - | - | /boot | xfs |  |
| sdd3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sdd4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sdd5 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 1550 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 1.92 TB (No Raid) | sda | sda1 | 5.238 TiB | vg\_data | lv\_data | /data | xfs |  |
| 3 | 01 x 1.92 TB (No Raid) | sdb | sdb1 |
| 4 | 01 x 1.92 TB (No Raid) | sdc | sdc1 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

| **Thông số** | **Value** |
| --- | --- |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các tham số khác:

|  |  |  |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| Disable CPU frequency scaling | *for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done* | Disable CPU frequency scaling |
| *zone\_reclaim\_mode* | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | *sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab*  *sudo swapoff –all* | Disable swap |
| Optimize SSDs |  |  |
| */sys/block/device\_name/queue/schedu* | *deadline* | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| */sys/block/device\_name/queue/nr\_requests* | *128* | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| */sys/class/block/device\_name/queue/rotational* | *0* |  |
| */sys/class/block/device\_name/queue/read\_ahead\_kb* | *8* |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Thông số User và CSDL

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| mtt\_adhoc | mtt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng MTT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| mtt\_app | mtt\_app | ks\_mtt\_system.mtt\_service\_config | SELECT |
| mtt\_category | mtt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_mtt\_system ks\_dangky | SELECT, UPDATE |
| mtt\_config | mtt\_config | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_delegation | mtt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_examination | mtt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| mtt\_explanation | mtt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| mtt\_explanation\_tvan | mtt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice | mtt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice\_code | mtt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| mtt\_invoice\_code\_adhoc | mtt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| mtt\_job | mtt\_job | ks\_mtt\_system | SELECT |
| mtt\_job\_config | mtt\_job\_config | ks\_mtt\_system ks\_danhmuc | SELECT, UPDATE |
| mtt\_message | mtt\_message | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_query | mtt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration | mtt\_registration | ks\_mtt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration\_status | mtt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| mtt\_security\_official | mtt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_security\_taxpayer | mtt\_security\_taxpayer | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_sync | mtt\_sync | ks\_danhmuc | SELECT, UPDATE |
| mtt\_system | mtt\_system | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_tax\_risk | mtt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_expired | mtt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_status | mtt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tvan\_status | mtt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_verification | mtt\_verification | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_mtt\_to\_dwh\_ods | job\_mtt\_to\_dwh\_ods | ks\_dangky.mtt\_dky  ks\_dangky.mtt\_tkhai  ks\_hoadon.mtt\_bthctiet\_mgr  ks\_hoadon.mtt\_bthop  ks\_hoadon.mtt\_hdhhdvu  ks\_hoadon.mtt\_hdon  ks\_hoadon.mtt\_tbhgthdon  ks\_hoadon.mtt\_tbssdt  ks\_hosogoc.mtt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_mtt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
| 2 | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 8443, 8888, 61620 :TCP | 1 | Mở cổng từ các DSE node đến máy chủ quản trị DSE OpsCenter | Vĩnh viễn |
| 3 | 10.64.211.14,  10.64.211.12, 10.64.211.11 | Máy chủ Terminal | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 22,4040,5598,5599,7080,7081,8983,9042,9142,9091,9077,9999,18080:TCP | 1 | Mở cổng từ Remote client tới các DSE node | Vĩnh viễn |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 | Dashboard Grafana | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 10.64.212.206 => 10.64.212.208 | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP),  10.64.98.112 --> 10.64.98.121 | HDDT Core Microservice | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Docs | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Docs | Vĩnh viễn |
| 3 | 10.64.90.153 => 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (DR\_Docs) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Docs | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.161.209=> 10.64.161.212 | Máy chủ DSE XML mới (MTT DR\_Docs) | 10.64.102.201 => 10.64.102.218,  10.64.161.201 => 10.64.161.207 | DSE (MTT DC\_Docs, DR\_Docs) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ XML cũ sang các máy chủ XML mới | Vĩnh viễn |

#### Thông số chi tiết CSDL DOC

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Loại** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| Security | client\_encryption\_options | enabled TRUE |
| General | num\_tokens | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | 3 |
| tpc\_pending\_requests\_limit | 256 |
| tpc\_cores |  |
| Directory | data\_file\_directories | /data/data |
| commitlog\_directory | /commitlog |
| saved\_caches\_directory | /data/saved\_caches |
| Ports | native\_transport\_port\_ssl | 9142 |
| NodeSync | rate\_in\_kb | 10240 |
| Caches | row\_cache\_size\_in\_mb | 500 |
| row\_cache\_save\_period | 36000 |
| Timeouts | read\_request\_timeout\_in\_ms | 5000 |
| write\_request\_timeout\_in\_ms | 2000 |
| stream\_outbound\_permits\_in\_mb | 8 |
| input\_stream\_channel\_timeout\_in\_ms | 432000000 |
| Snapshots | incremental\_backups | TRUE |
| auto\_snapshot | TRUE |
| Hinted Handoff | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hints\_delivery\_threads | 6 |
| hints\_directory | /data/hints |
| Change Data Capture | cdc\_raw\_directory | /data/cdc\_raw |
| Miscellaneous | metadata\_directory | /data/metadata |
| Cluster Communication | endpoint\_snitch | GossipingPropertyFileSnitch |
| zerocopy\_streaming\_enabled | FALSE |

* Thông số File dse.yaml:

| **Loại** | **Tham số** | **Tham số thành phần** | **Giá trị** |
| --- | --- | --- | --- |
| DSE Authorizer Options | authorization\_options | enabled | TRUE |
| transitional\_mode | disabled |
| allow\_row\_level\_security | FALSE |
| DSE Metrics Collector | insights\_options | data\_dir | /data/insights |
| log\_dir | /u01/log/dse/insights |
| Encryption Settings | system\_key\_directory |  | /u01/app/dse/conf |
| Audit Logging Settings | audit\_logging\_options | enabled | TRUE |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| Miscellaneous | internode\_messaging\_options | client\_max\_connections | 200 |
| port | 8609 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

|  |  |  |
| --- | --- | --- |
| **THAM SỐ DR\_DOC** | | |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_DOC |  |
| Số lượng Node bổ sung | 4 |  |
| Workload | Cassandra |  |

##### Thông số Logical Rack

Logical Rack của DR\_Doc được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 01 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Doc:
* Số lượng node: 4
* Logical rack: 02
* Số lượng nodes trên logical rack dr\_doc1: 2
* Số lượng nodes trên logical rack dr\_doc2: 2
* Thông tin được hiển thị chi tiết theo bảng sau:

| **TT** | **DC** | **Tham số** | **Physical Rack** | | **Tổng** |
| --- | --- | --- | --- | --- | --- |
| **Rack D11** | |  |
| 1 | DR\_Doc 4 node (RF=2) | Chassis | 1 | | 1 |
| Nodes | 4 | | 4 |
| Logical Rack ID | dr\_doc1 | dr\_doc2 |  |

##### Thông số các Node CSDL DOC

Thông số cấu hình từng node CSDL XML như sau:

| **CẤU HÌNH TỪNG NODE DOC** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 \* 1,92TB SSD |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 5.2 TiB |  |
| DNS | 10.64.88.11 |  |
| 10.64.88.12 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Doc

| **THÔNG TIN CÁC KEYSPACE ỨNG DỤNG** | | |
| --- | --- | --- |
| **Tên keyspace** | **Chú thích** | **Keyspace replication Strategy** |
| ks\_hosogoc  (Hồ sơ gốc) | Phục vụ mục đích tra cứu thông tin hồ sơ gốc như: Tờ khai đăng ký, Thông báo, Hóa đơn gốc từ NNT gửi cho CQT. | NetworkTopologyStrategy |
| OpsCenter | Quản trị OpsCenter | NetworkTopologyStrategy |
| ks\_kad (Kafka) | Quản trị Kafka | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Doc, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Doc được phân bố theo bảng sau:

| **Keyspace** | **DR\_Doc** | **Keyspace replication Strategy** |
| --- | --- | --- |
| **ks\_hoadon** | 2 | NetworkTopologyStrategy |
| **ks\_danhmuc** | 2 | NetworkTopologyStrategy |
| **ks\_dangky** | 2 | NetworkTopologyStrategy |
| **ks\_hddt\_system** | 2 | NetworkTopologyStrategy |
| **ks\_luutam** | 2 | NetworkTopologyStrategy |
| **ks\_tdt\_system** | 2 | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL DOC tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 10 phút kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Mỗi máy chủ được cấu hình log với dung lượng không quá 500Mb hoặc thời gian lưu trữ không quá 6 tháng.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.158 | 9997 |
| 10.64.212.159 | 9997 |
| 10.64.212.213 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.215 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |

### Thiết kế chi tiết hệ thống máy chủ Ana

#### Thiết kế hạ tầng vật lý

Hệ thống CSDL Anna được bổ sung tạm thời (phục vụ chuyển đổi DC sang DC mới) 4 node được cài đặt trên các máy chủ mật độ cao Dell PowerEdge C6620. Một Chassis Dell PowerEdge C6600 2U được lắp đặt 04 máy chủ Dell PowerEdge C6620. Mỗi máy chủ Dell PowerEdge C6620 có 04 kết nối tốc độ 10Gb với hệ thống chuyển mạch dữ liệu (Data Switch) cung cấp các kết nối Data.

Để đảm bảo tính dự phòng thì 04 cổng 10Gbps sẽ được cắm trên trên 2 switch chuyển mạch dữ liệu khác nhau. Các port sẽ được cấu hình giao thức LACP trên switch và cấu hình Bonding trên hệ điều hành Linux để đảm bảo tăng tốc độ băng thông cũng như tính dự phòng.

##### Phân bổ tài nguyên máy chủ

| **Site** | Trung tâm dữ liệu dự phòng |
| --- | --- |
| **Tên DC​** | DR\_Ana |
| **Số lượng Node bổ sung tại DC​** | 4 |
| **Workload​** | Analytics + Search ​​ |

##### Bảng phân bổ lắp đặt Rack

* Các máy chủ CSDL Ana được phân bổ trên 01 Rack vật lý như sau:

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Rack A11** | **Công suất cực đại (W)** | **Công suất hiệu dụng (W) P = Pmax x 80%** | **C19** | **Công suất lạnh (BTU)** | **Cân nặng (Kg)** |
| A11 | U10-U11 | dri-ehdanac6600ch14 | 1900 | 1520 | 2 | 4772.8 | 43 |

* Bảng lắp đặt các máy chủ CSDL XML trên Rack chi tiết như sau:

| **STT** | **Rack** | **U** | **Chassis** | **Host** |
| --- | --- | --- | --- | --- |
| 1 | A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 |
| 2 | dri-ehdmttanadb206 |
| 3 | dri-ehdmttanadb207 |
| 4 | dri-ehdmttanadb208 |

##### Sơ đồ lắp đặt trên tủ Rack

Sơ đồ lắp đặt trên tủ rack được bố trí như sau:

A list of numbers and letters

Description automatically generated

##### Thông tin kết nối quản trị phần cứng

Quản trị phần cứng của các máy chủ được kết nối như sau:

A diagram of a computer server

Description automatically generated

Hình 8: Kết nối quản trị máy chủ Ana

Thông tin IP quản trị của máy chủ CSDL Ana được thể hiện chị tiết qua bảng sau:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **No.** | **Chassis** | **Device** | **VLAN** | **IP iDRAC** | **Netmask** | **GateWay** |
| 1 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 | 309 | 10.64.170.223 | 255.255.255.0 | 10.64.170.1 |
| 2 |  | dri-ehdmttanadb206 | 309 | 10.64.170.224 | 255.255.255.0 | 10.64.170.1 |
| 3 |  | dri-ehdmttanadb207 | 309 | 10.64.170.225 | 255.255.255.0 | 10.64.170.1 |
| 4 |  | dri-ehdmttanadb208 | 309 | 10.64.170.226 | 255.255.255.0 | 10.64.170.1 |

##### Thông tin kết nối IP máy chủ

Thông tin chi tiết IP máy chủ CSDL Ana được thể hiện ở bảng sau:

| **No.** | **Chassis** | **Device** | **VLAN** | **IP Data** | **Netmask** | **GateWay** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 | 234 | 10.64.160.205 | 255.255.255.0 | 10.64.159.1 |
| 2 |  | dri-ehdmttanadb206 | 234 | 10.64.160.206 | 255.255.255.0 | 10.64.159.1 |
| 3 |  | dri-ehdmttanadb207 | 234 | 10.64.160.207 | 255.255.255.0 | 10.64.159.1 |
| 4 |  | dri-ehdmttanadb208 | 234 | 10.64.160.208 | 255.255.255.0 | 10.64.159.1 |

##### Thông tin kết nối máy chủ

- Trên mỗi máy chủ (node) của hệ thống máy chủ CSDL ANA có 04 cổng ethernet quang 10Gbps. Để đảm bảo dự phòng mức vật lý, 4 port của máy chủ sẽ kết nối đến 2 Switch khác nhau, mỗi Switch cắm 2 port. Các port này sau đó sẽ được cấu hình thức LACP để tăng tốc độ cũng như tính dự phòng.

- Sơ đồ kết nối mạng máy như sau:

A diagram of a computer server

Description automatically generated

*Mô hình kết nối máy chủ CSDL ANA*

Thông tin chi tiết kết nối máy chủ được thể hiện chi tiết qua bảng sau:

| **Vị trí mới tại DR)** | | | |  |  |  | **TO Switch DR** | | | | **Mode** | **Vlan ID** | **Type** | **Cable Speed** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Rack** | **U** | **Chassis** | **Device** | **Port** | **LACP** | **Logical Interface** | **Rack** | **U** | **Switch / Device** | **Port** |  |  |  |  |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/26 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/15 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb205 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb206 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/27 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb206 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/16 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb206 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb207 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/28 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb207 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/17 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb207 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb208 | iDRAC |  |  | A01 | U25 | DR-MGMT-ACCSW08 | ge-0/0/29 | Access | 309 | MGMT | Đồng - 1Gb |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb208 | P1 | Active | bond0 | D01 | U33 | DR-INT-ACCSW-12 | Eth1/18 | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |
| A11 | U10-U11 | dri-ehdanac6600ch14 | dri-ehdmttanadb208 | P2 | Active |  |  |  |  | Trunk | 232, 233, 234, 235 | Data | Quang - 10G |

#### Thiết kế thông số hệ điều hành

##### Thông số các máy chủ CSDL Ana

Bảng thông số các máy chủ CSDL Ana như sau:

| **STT** | **Hostname** | **OS** | **CPU** | **RAM (GB)** | **HDD (GB)** | **IP** |
| --- | --- | --- | --- | --- | --- | --- |
| 1 | dri-ehdmttanadb205 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.160.205 |
| 2 | dri-ehdmttanadb206 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.160.206 |
| 3 | dri-ehdmttanadb207 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.160.207 |
| 4 | dri-ehdmttanadb208 | RHEL 8.10 | 24 | 128 | 4\*960 | 10.64.160.208 |

Thông số cấu hình các dịch vụ mạng

|  |  |
| --- | --- |
| DNS Server | 10.64.88.11, 10.64.88.12 |
| NTP Server | 10.64.68.26 |

##### Danh sách các gói cài đặt OS

Danh sách các gói cài đặt hệ điều hành như sau:

| **Gói phần mềm** | **Package name** |
| --- | --- |
| Java | OpenJDK 8 (1.8.0\_432) |
| Hỗ trợ CSDL | python-2.7, wget, curl, unzip |
| Python | 2.7.x |
| Đồng bộ NTP Time Server | chrony (cấu hình NTP của TCT)  IP NTP: 10.64.68.26 |
| Công cụ monitor, debug, khác | telnet wget net-tools hdparm iotop iftop nfs-utils rsync sshpass pssh sysstat dstat htop unzip |

##### Thông số Mountpoint

* Nguyên tắc cấu hình ổ cứng lưu trữ:
* Máy chủ CSDL sử dụng ổ cứng local để cài đặt HĐH và lưu trữ dữ liệu của CSDL.
* Để giữ nguyên mode của card quản trị ổ cứng (RAID card) các ổ cứng sẽ được tạo một array raid 0 và chứa 1 ổ cứng tương ứng.
* Chi tiết các mount point được quy hoạch như sau:

| **STT** | **Hard Disk** | | **PV** | **Dung lượng** | **Volume Group** | **Logicalal Volume** | **Mount point** | **Định dạng** | **Note** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| 1 | 01 x 960 GB (RAID 0) | sda | sda1 | 600 MiB | - | - | /boot/efi | efi |  |
| sda2 | 1 GiB | - | - | /boot | xfs |  |
| sda3 | 100 GiB | vg\_root | lv\_root | / | xfs |  |
| 8 GiB | lv\_swap |  | swap |  |
| sda4 | 20 GiB | vg\_commitlog | lv\_commitlog | /commitlog | xfs |  |
| sda6 | 100 GiB | vg\_u01 | lv\_u01 | /u01 | xfs |  |
| Free | 664 GiB |  |  |  |  | dự phòng |
| 2 | 01 x 960 GB (No Raid) | sdb | sdb1 | 650 GiB | vg\_solr | lv\_solr | /solr\_index | xfs |  |
| Free | 224 GiB |  |  |  |  | dự phòng |
| 3 | 01 x 960 GB (No Raid) | sdc | sdc1 | 1.746 TiB | vg\_data | lv\_data | /data | xfs |  |
| 4 | 01 x 960 GB (No Raid) | sdd | sdd1 |

##### Thông số Kernel

1. Thêm các cấu hình sau vào file **/etc/sysctl.conf**: thay thế các giá trị đang lấy mặc định:

| **Kernel parameter** | **Value** | **Diễn giải** |
| --- | --- | --- |
| net.ipv4.tcp\_keepalive\_time | 60 | Khoảng thời gian giữa gói dữ liệu cuối cùng được gửi và gói keepalive thăm dò đầu tiên (giây) |
| net.ipv4.tcp\_keepalive\_probes | 3 | Số lượng gói thăm dò được gửi và không được xác nhận trước khi client cho rằng kết nối bị mất và thông báo cho lớp ứng dụng (giây) |
| net.ipv4.tcp\_keepalive\_intvl | 10 | Khoảng thời gian giữa các gói thăm dò (giây) |
| net.core.rmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket nhận (byte) |
| net.core.wmem\_max | 16777216 | Kích thước buffer tối đa của toàn bộ các socket gửi (byte) |
| net.core.rmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket nhận (byte) |
| net.core.wmem\_default | 16777216 | Kích thước buffer mặc định của toàn bộ các socket gửi (byte) |
| net.core.optmem\_max | 40960 | Tăng số lượng bộ nhớ đệm tùy chọn tối đa (byte) |
| net.ipv4.tcp\_rmem | 4096 87380 16777216 | Tăng không gian bộ đệm đọc được phân bổ (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| net.ipv4.tcp\_wmem | 4096 65536 16777216 | Tăng phân bổ không gian bộ đệm ghi (kích thước nhỏ nhất, kích thước khởi tạo, kích thước tối đa) (byte) |
| vm.max\_map\_count | 1048575 | Số vùng memory map tối đa mà một tiến trình có thể có |

1. **Set user resource limits(/etc/security/limits.conf)**

* Thiết lập user limit trên file **etc/security/limits.conf**:

| **Thông số** | **Value** | **Diễn giải** |
| --- | --- | --- |
| cassandra - memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user cassandra (KB) |
| cassandra - nofile | 1048576 | Số lượng file được mở tối đa của user cassandra |
| cassandra - nproc | 32768 | Số lượng process tối đa của user cassandra |
| cassandra - as | unlimited | Giới hạn không gian địa chỉ (address space) của user cassandra (KB) |
| rma soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user rma |
| rma hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user rma |
| \* soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của các user khác |
| \* hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của các user khác |
| \* soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của các user khác (KB) |
| \* hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của các user khác (KB) |
| \* soft memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| \* hard memlock | unlimited | Không gian địa chỉ (address space) lock-in-memory tối đa của user khác (KB) |
| root soft nofile | 1048576 | Giới hạn mềm (soft limit) số lượng file được mở tối đa của user root |
| root hard nofile | 1048576 | Giới hạn cứng (hard limit) số lượng file được mở tối đa của user root |
| root soft memlock | unlimited | Giới hạn mềm không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root hard memlock | unlimited | Giới hạn cứng không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root soft as | unlimited | Giới hạn mềm không gian địa chỉ (address space) của user root (KB) |
| root hard as | unlimited | Giới hạn cứng không gian địa chỉ (address space) của user root (KB) |
| root - memlock | unlimited | Giới hạn không gian địa chỉ (address space) lock-in-memory tối đa của user root |
| root - nofile | 1048576 | Số lượng file được mở tối đa của user root |
| root - nproc | 32768 | Số lượng process tối đa của user root |
| root - as | unlimited | Giới hạn không gian địa chỉ (address space) của user root (KB) |

* Thông số limit của user cassandra trên file cấu hình **cassandra.conf** tại đường dẫn **/etc/security/limits.d/**:

| **Thông số** | **Value** |
| --- | --- |
| cassandra - memlock | unlimited |
| cassandra - nofile | 1048576 |
| cassandra - nproc | 32768 |
| cassandra - as | unlimited |

Các tham số khác:

|  |  |  |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| Disable CPU frequency scaling | *for CPUFREQ in /sys/devices/system/cpu/cpu\*/cpufreq/scaling\_governor; do [ -f $CPUFREQ ] || continue; echo -n performance > $CPUFREQ; done* | Disable CPU frequency scaling |
| *zone\_reclaim\_mode* | 0 | Vô hiệu hóa zone\_reclaim\_mode |
| Disable swap | *sed -i 's/^\(.\*swap\)/#\1/' /etc/fstab*  *sudo swapoff –all* | Disable swap |
| Optimize SSDs |  |  |
| */sys/block/device\_name/queue/schedu* | *deadline* | Đặt IO schedule thành deadline cho mỗi ổ đĩa lưu dữ liệu DSE |
| */sys/block/device\_name/queue/nr\_requests* | *128* | Đặt giá trị nr\_request để cho biết số lượng yêu cầu đọc và ghi tối đa có thể được xếp hàng đợi |
| */sys/class/block/device\_name/queue/rotational* | *0* |  |
| */sys/class/block/device\_name/queue/read\_ahead\_kb* | *8* |  |
| NTP Server | server 10.64.68.26 iburst |  |

##### Thông số User và CSDL

Bảng chi tiết quy hoạch user như sau:

| **User** | **Group** | **Phòng quản lý** | **Mô tả** | **Thiết lập** | **User ID** | **Group ID** |
| --- | --- | --- | --- | --- | --- | --- |
| **User quản trị** | | | | | | |
| root | root | P4 | - Người dùng gốc mặc định, có quyền cao nhất | - Không cho phép SSH trực tiếp |  |  |
| sysadm | hddt wheel | P4 | - User quản trị của P4, có quyền sudo | - Cho phép SSH trực tiếp | 5001 | 5001 |
| backupadm | bkadm | P3 | - User quản trị backup của P3, phân quyền trên các thư mục theo user dbadmin để xử lý log. | - Cho phép SSH trực tiếp | 5003 | 5003 |
| dbadm | dbadmin  wheel | P2 | - User quản trị CSDL của P2, có quyền chạy sudo không cần nhập lại mật khẩu | - Cho phép SSH trực tiếp | 5002 | 5002 |
| rma | rma |  | User monitor các máy DSE từ Host monitor và OpsCenter | - Cho phép SSH trực tiếp | 6001 | 6001 |
| monitor | monitor | NOC | - User vận hành, giám sát hệ thống | - Cho phép SSH trực tiếp | 6002 | 6002 |
| **User theo ứng dụng** | | | | | | |
| node\_exporter | node\_exporter | P4 | User khởi chạy ứng dụng node\_exporter, đẩy metric lên Grafana | - Không cho phép SSH trực tiếp  - Thư mục phân quyền:  /u01/HDDT/node\_exporter | 7001 | 7001 |
| cassandra | cassandra  bkadm | P2 | Super user của DSE, tự sinh ra khi cài đặt | - Không cho phép SSH trực tiếp |  |  |
| splunk | splunk | P4 | User monitor splunk | Thư mục phân quyền:  /u01/splunkforwarder | 7002 | 7002 |

* Quy hoạch role trên CSDL DSE:

| **STT** | **Role** | **Login** | **Superuser** | **Mô tả** |
| --- | --- | --- | --- | --- |
| 1 | superuser | YES | YES | Người dùng mặc định sinh ra khi cài đặt phần mềm. |
| 2 | super\_admin | YES | YES | Có quyền CREATE KEYSPACE và DROP KEYSPACE, cũng như tất cả các quyền trong đối tượng con bao gồm: CREATE, ALTER, AUTHORIZE, DESCRIBE, DROP, MODIFY, và SELECT. |
| 4 | noc | YES | NO | Các người dùng có quyền LOGIN, SELECT, UPDATE các đối tượng được cấp phép để monitor. |
| 5 | trienkhai/hotro/quantri | YES | NO | Dành cho đối tác triển khai, hỗ trợ, quản trị db. Tài khoản chỉ cấp trong thời gian thực hiện hđ, dự án |
| 6 | appsupport | YES | NO | Cán bộ thuế hỗ trợ ứng dụng. |

* Quy hoạch các user trên CSDL DSE:

| **User** | **Role** | **Keyspace** | **Permission** | **Mô tả** |
| --- | --- | --- | --- | --- |
| mtt\_adhoc | mtt\_adhoc | ks\_dangky ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE | Các account dành cho service ứng dụng MTT kết nối tới db, có các quyền LOGIN, SELECT, UPDATE trên các keyspaces ứng dụng được cấp phép. |
| mtt\_app | mtt\_app | ks\_mtt\_system.mtt\_service\_config | SELECT |
| mtt\_category | mtt\_category | ks\_danhmuc ks\_hosogoc ks\_hoadon ks\_mtt\_system ks\_dangky | SELECT, UPDATE |
| mtt\_config | mtt\_config | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_delegation | mtt\_delegation | ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_examination | mtt\_examination | ks\_hoadon ks\_danhmuc | SELECT, UPDATE |
| mtt\_explanation | mtt\_explanation | ks\_hosogoc ks\_hoadon ks\_luutam | SELECT, UPDATE |
| mtt\_explanation\_tvan | mtt\_explanation\_tvan | ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice | mtt\_invoice | ks\_hoadon  ks\_luutam  ks\_dangky  ks\_hosogoc | SELECT, UPDATE |
| mtt\_invoice\_code | mtt\_invoice\_code | ks\_hoadon ks\_hosogoc ks\_luutam | SELECT, UPDATE |
| mtt\_invoice\_code\_adhoc | mtt\_invoice\_code\_adhoc | ks\_hoadon ks\_hosogoc ks\_dangky ks\_luutam | SELECT, UPDATE |
| mtt\_job | mtt\_job | ks\_mtt\_system | SELECT |
| mtt\_job\_config | mtt\_job\_config | ks\_mtt\_system ks\_danhmuc | SELECT, UPDATE |
| mtt\_message | mtt\_message | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| mtt\_query | mtt\_query | ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration | mtt\_registration | ks\_mtt\_system ks\_hoadon ks\_dangky ks\_hosogoc | SELECT, UPDATE |
| mtt\_registration\_status | mtt\_registration\_status | ks\_dangky | SELECT, UPDATE |
| mtt\_security\_official | mtt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_security\_taxpayer | mtt\_security\_taxpayer | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_sync | mtt\_sync | ks\_danhmuc | SELECT, UPDATE |
| mtt\_system | mtt\_system | ks\_mtt\_system | SELECT, UPDATE |
| mtt\_tax\_risk | mtt\_tax\_risk | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_expired | mtt\_tin\_expired | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tin\_status | mtt\_tin\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_tvan\_status | mtt\_tvan\_status | ks\_danhmuc | SELECT, UPDATE |
| mtt\_verification | mtt\_verification | ks\_mtt\_system ks\_hoadon ks\_hosogoc | SELECT, UPDATE |
| job\_mtt\_to\_dwh\_ods | job\_mtt\_to\_dwh\_ods | ks\_dangky.mtt\_dky  ks\_dangky.mtt\_tkhai  ks\_hoadon.mtt\_bthctiet\_mgr  ks\_hoadon.mtt\_bthop  ks\_hoadon.mtt\_hdhhdvu  ks\_hoadon.mtt\_hdon  ks\_hoadon.mtt\_tbhgthdon  ks\_hoadon.mtt\_tbssdt  ks\_hosogoc.mtt\_hsg\_hdon | SELECT |
| spark\_jobserver | spark\_jobserver | spark\_jobserver | CREATE, ALTER, DROP, SELECT, AUTHORIZE, DESCRIBE, UPDATE, TRUNCATE | User cho SPARK jobs server có toàn quyền trên keyspace spark\_jobserver |
| spark\_jobserver\_startup | spark\_jobserver\_startup | HiveMetaStore.sparkmetastore  dsefs.locks  ks\_baocao  ks\_dangky  ks\_danhmuc  ks\_hoadon  system.size\_estimates | SELECT |
| tdt\_config | tdt\_config | ks\_tdt\_system | SELECT | Account dành cho service ứng dụng Tem điện tử kết nối đến DB, có quyền LOGIN, SELECT, UPDATE trên các đối tượng được cấp phép |
| tdt\_security\_official | tdt\_security\_official | ks\_mtt\_system | SELECT, UPDATE |
| tdt\_system\_official | tdt\_system\_official | ks\_mtt\_system | SELECT, UPDATE |

##### Danh sách yêu cầu mở port

Thông tin cấu hình mở port chi tiết như bảng sau:

| **STT** | **Địa chỉ nguồn** | | **Địa chỉ đích** | | **Port** | **Số chiều** | **Mục đích sử dụng** | **Thời hạn** |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **IP** | **Description** | **IP** | **Description** |
|  | **Mở cổng giữa node DSE và OpsCenter** | | | | | | | |
| 1 | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 22,7080,9042,9142,61621:TCP | 1 | Mở cổng từ máy chủ quản trị DSE OpsCenter đến các DSE node | Vĩnh viễn |
| 2 | 10.64.161.143=> 10.64.161.146 | Máy chủ DSE XML mới (DR\_Ana) | 10.64.99.2, 10.64.99.3 | Máy chủ OpsCenter | 8443, 8888, 61620 :TCP | 1 | Mở cổng từ các DSE node đến máy chủ quản trị DSE OpsCenter | Vĩnh viễn |
| 3 | 10.64.211.14,  10.64.211.12, 10.64.211.11 | Máy chủ Terminal | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 22,4040,5598,5599,7080,7081,8983,9042,9142,9091,9077,9999,18080:TCP | 1 | Mở cổng từ Remote client tới các DSE node | Vĩnh viễn |
|  | **Mở cổng giữa node DSE và hệ thống giám sát** | | | | | | | |
| 1 | 10.64.212.209 => 10.64.212.211 | Dashboard Grafana | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 9100:TCP | 1 | Mở cổng từ máy giám sát Dashboard Grafana tới các DSE node | Vĩnh viễn |
| 2 | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (DR\_Ana) | 10.64.212.206 => 10.64.212.208 | HDDT Logging ELK | 9411: TCP | 1 | Mở cổng từ các DSE node tới máy chủ quản lý log tập trung ELK | Vĩnh viễn |
|  | **Mở cổng giữa App HDDT và DSE node mới** | | | | | | | |
| 1 | 10.64.98.36 => 10.64.98.40 (5 IP ), 10.64.98.186 => 10.64.98.199 (14 IP), 10.64.98.202 => 10.64.98.254 (53 IP),  10.64.98.112 🡪 10.64.98.121 | HDDT Core Microservice | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Core Microservice đến DC\_Docs | Vĩnh viễn |
| 2 | 10.64.90.151, 10.64.90.152 | HDDT Config | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Config đến DC\_Docs | Vĩnh viễn |
| 3 | 10.64.90.153 => 10.64.90.156 (4 IP) | HDDT Registry and Discovery | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (MTT DR\_Ana) | 9042, 9142: TCP | 1 | Mở cổng từ hệ thống HDDT Registry and Discovery đến DC\_Docs | Vĩnh viễn |
|  | **Mở cổng giữa DSE node hiện tại và DSE node mới phục vụ đồng bộ** | | | | | | | |
| 1 | 10.64.160.205=> 10.64.160.208 | Máy chủ DSE Ana mới (DR\_Ana) | 10.64.101.200 => 10.64.101.205,  10.64.160.200=> 10.64.160.203 | DSE (MTT DC\_Ana, DR\_Ana) | 9042, 9142: TCP | 2 | Replicate dữ liệu từ các máy chủ XML cũ sang các máy chủ XML mới | Vĩnh viễn |

#### Thông số chi tiết CSDL Ana

##### Danh sách các gói cài đặt DSE

| **CẤU HÌNH TỪNG NODE** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| DSE Version | DSE 6.8.47 |  |
| User:group service | cassandra:cassandra |  |
| Các gói cài đặt | dse-libcassandra-6.8.47-1.noarch |  |
| dse-libgraph-6.8.47-1.noarch |
| dse-libhadoop2-client-6.8.47-1.noarch |
| dse-6.8.47-1.noarch |
| dse-libtomcat-6.8.47-1.noarch |
| dse-libspark-6.8.47-1.noarch |
| dse-full-6.8.47-1.noarch |
| dse-liblog4j-6.8.47-1.noarch |
| dse-libsolr-6.8.47-1.noarch |

##### Thông tin cài đặt DSE

| **STT** | **Thư mục** | **Mô tả** |
| --- | --- | --- |
| 1 | /etc/dse/cassandra/cassandra.yaml | cassandra.yaml là tệp cấu hình chính cho Cassandra database. |
| 2 | /etc/dse/dse.yaml | dse.yaml là tệp cấu hình chính cho DataStax Enterprise |
| 3 | /data/ | Thư mục lưu trữ: |
| - data |
| - hints |
| - saved\_caches |
| - metadata |
| - insight\_data |
| 4 | /commitlog | Thư mục lưu trữ commitlog |
| 5 | /u01/log/dse/cassandra | Thư mục lưu trữ log files, bao gồm: |
| - thư mục audit |
| - debug.log |
| - system.log |
| - … |
| 6 | /usr/share/dse/cassandra | Các cài đặt môi trường. |
| 7 | /usr/share/dse/cassandra/tools | Các công cụ để kiểm tra, khởi động, sử dụng SSTables, YAML. |
| 8 | /etc/dse/cassandra | Các file thuộc tính và cqlshrc mẫu: |
| - cassandra-env.sh |
| - cassandra-rackdc.properties |
| - cassandra-topology.properties |
| - cassandra-topology.yaml |
| - commitlog\_archiving.properties |
| - cqlshrc.sample |
| - logback.xml |
| 9 | /etc/init.d | Đặt node type và cấu hình khác. |
| 10 | /usr/share/dse/solr | Thư mục chứa solr configuration |
| 11 | /etc/dse/cassandra/logback.xml | logback.xml là file cấu hình log của DSE |
| 12 | /u01/log/dse/cassandra/audit/dropped\_audit\_events.log | Thư mục chứa dropped events logs. |

##### Thông số các file cấu hình DSE

* Thông số File cassandra.yaml:

| **Tên tham số** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| permissions\_cache\_max\_entries | permissions\_cache\_max\_entries | 1000 |
| ssl\_storage\_port | ssl\_storage\_port | 7001 |
| guardrails | guardrails |  |
| batch\_size\_fail\_threshold\_in\_kb | 640 |
| tombstone\_warn\_threshold | 1000 |
| tombstone\_failure\_threshold | 100000 |
| disk\_usage\_max\_disk\_size\_in\_gb | -1 |
| batch\_size\_warn\_threshold\_in\_kb | 64 |
| partition\_size\_warn\_threshold\_in\_mb | 100 |
| storage\_port | storage\_port | 7000 |
| backup\_service | backup\_service |  |
| enabled | FALSE |
| continuous\_paging | continuous\_paging |  |
| max\_concurrent\_sessions | 240 |
| max\_session\_pages | 4 |
| max\_page\_size\_mb | 8 |
| max\_local\_query\_time\_ms | 5000 |
| client\_timeout\_sec | 600 |
| cancel\_timeout\_sec | 5 |
| paused\_check\_interval\_ms | 1 |
| batchlog\_replay\_throttle\_in\_kb | batchlog\_replay\_throttle\_in\_kb | 1024 |
| commit\_failure\_policy | commit\_failure\_policy | stop |
| native\_transport\_max\_frame\_size\_in\_mb | native\_transport\_max\_frame\_size\_in\_mb | 256 |
| commitlog\_segment\_size\_in\_mb | commitlog\_segment\_size\_in\_mb | 32 |
| memtable\_flush\_writers | memtable\_flush\_writers | 8 |
| allocate\_tokens\_for\_local\_replication\_factor | allocate\_tokens\_for\_local\_replication\_factor | 2 |
| client\_encryption\_options | client\_encryption\_options |  |
| truststore | /etc/dse/keystores/client.truststore |
| protocol | TLS |
| optional | FALSE |
| require\_client\_auth | FALSE |
| enabled | TRUE |
| truststore\_password | cassandra |
| algorithm | SunX509 |
| keystore | /etc/dse/keystores/client.keystore |
| truststore\_type | JKS |
| keystore\_type | JKS |
| keystore\_password | cassandra |
| inter\_dc\_tcp\_nodelay | inter\_dc\_tcp\_nodelay | FALSE |
| column\_index\_cache\_size\_in\_kb | column\_index\_cache\_size\_in\_kb | 2 |
| internode\_authenticator | internode\_authenticator | org.apache.cassandra.auth.AllowAllInternodeAuthenticator |
| max\_value\_size\_in\_mb | max\_value\_size\_in\_mb | 256 |
| authorizer | authorizer | com.datastax.bdp.cassandra.auth.DseAuthorizer |
| num\_tokens | num\_tokens | 8 |
| listen\_on\_broadcast\_address | listen\_on\_broadcast\_address | FALSE |
| row\_cache\_save\_period | row\_cache\_save\_period | 36000 |
| row\_cache\_class\_name | row\_cache\_class\_name | org.apache.cassandra.cache.OHCProvider |
| native\_transport\_allow\_older\_protocols | native\_transport\_allow\_older\_protocols | TRUE |
| disk\_failure\_policy | disk\_failure\_policy | stop |
| native\_transport\_port | native\_transport\_port | 9042 |
| enable\_user\_defined\_functions\_threads | enable\_user\_defined\_functions\_threads | TRUE |
| server\_encryption\_options | server\_encryption\_options |  |
| internode\_encryption | none |
| dynamic\_snitch\_reset\_interval\_in\_ms | dynamic\_snitch\_reset\_interval\_in\_ms | 600000 |
| compaction\_throughput\_mb\_per\_sec | compaction\_throughput\_mb\_per\_sec | 64 |
| data\_file\_directories | data\_file\_directories | /data/data |
| role\_manager | role\_manager | com.datastax.bdp.cassandra.auth.DseRoleManager |
| leaks\_detection\_params | leaks\_detection\_params |  |
| sampling\_probability | 0,01 |
| max\_stacks\_cache\_size\_mb | 32 |
| num\_access\_records | 0 |
| max\_stack\_depth | 30 |
| column\_index\_size\_in\_kb | column\_index\_size\_in\_kb | 16 |
| windows\_timer\_interval | windows\_timer\_interval | 1 |
| rpc\_keepalive | rpc\_keepalive | TRUE |
| commitlog\_total\_space\_in\_mb | commitlog\_total\_space\_in\_mb | 8192 |
| nodesync | nodesync |  |
| rate\_in\_kb | 10240 |
| snapshot\_before\_compaction | snapshot\_before\_compaction | FALSE |
| tracetype\_query\_ttl | tracetype\_query\_ttl | 86400 |
| native\_transport\_port\_ssl | native\_transport\_port\_ssl | 9142 |
| pick\_level\_on\_streaming | pick\_level\_on\_streaming | TRUE |
| system\_keyspaces\_filtering | system\_keyspaces\_filtering | FALSE |
| row\_cache\_size\_in\_mb | row\_cache\_size\_in\_mb | 500 |
| tracetype\_repair\_ttl | tracetype\_repair\_ttl | 604800 |
| auto\_bootstrap | auto\_bootstrap | TRUE |
| commitlog\_sync | commitlog\_sync | periodic |
| concurrent\_validations | concurrent\_validations | 0 |
| disk\_optimization\_strategy | disk\_optimization\_strategy | ssd |
| counter\_cache\_save\_period | counter\_cache\_save\_period | 7200 |
| emulate\_dbaas\_defaults | emulate\_dbaas\_defaults | FALSE |
| user\_defined\_function\_warn\_micros | user\_defined\_function\_warn\_micros | 500 |
| back\_pressure\_enabled | back\_pressure\_enabled | FALSE |
| user\_defined\_function\_fail\_micros | user\_defined\_function\_fail\_micros | 10000 |
| slow\_query\_log\_timeout\_in\_ms | slow\_query\_log\_timeout\_in\_ms | 500 |
| trickle\_fsync | trickle\_fsync | TRUE |
| streaming\_keep\_alive\_period\_in\_secs | streaming\_keep\_alive\_period\_in\_secs | 300 |
| io\_global\_queue\_depth | io\_global\_queue\_depth | 128 |
| write\_request\_timeout\_in\_ms | write\_request\_timeout\_in\_ms | 2000 |
| initial\_token | initial\_token | null |
| incremental\_backups | incremental\_backups | TRUE |
| truncate\_request\_timeout\_in\_ms | truncate\_request\_timeout\_in\_ms | 60000 |
| snapshot\_before\_dropping\_column | snapshot\_before\_dropping\_column | FALSE |
| enable\_scripted\_user\_defined\_functions | enable\_scripted\_user\_defined\_functions | FALSE |
| read\_request\_timeout\_in\_ms | read\_request\_timeout\_in\_ms | 5000 |
| request\_timeout\_in\_ms | request\_timeout\_in\_ms | 10000 |
| start\_native\_transport | start\_native\_transport | TRUE |
| back\_pressure\_strategy | back\_pressure\_strategy |  |
| - class\_name | org.apache.cassandra.net.RateBasedBackPressure |
| parameters |  |
| - high\_ratio | 0,9 |
| factor | 5 |
| flow | FAST |
| metadata\_directory | metadata\_directory | /data/metadata |
| concurrent\_materialized\_view\_builders | concurrent\_materialized\_view\_builders | 2 |
| memtable\_allocation\_type | memtable\_allocation\_type | offheap\_objects |
| saved\_caches\_directory | saved\_caches\_directory | /data/saved\_caches |
| transparent\_data\_encryption\_options | transparent\_data\_encryption\_options |  |
| enabled | FALSE |
| chunk\_length\_kb | 64 |
| cipher | AES/CBC/PKCS5Padding |
| key\_alias | testing:1 |
| internode\_compression | internode\_compression | dc |
| authenticator | authenticator | com.datastax.bdp.cassandra.auth.DseAuthenticator |
| phi\_convict\_threshold | phi\_convict\_threshold | 8 |
| max\_hints\_delivery\_threads | max\_hints\_delivery\_threads | 6 |
| cross\_node\_timeout | cross\_node\_timeout | FALSE |
| partitioner | partitioner | org.apache.cassandra.dht.Murmur3Partitioner |
| max\_pending\_lw\_transactions | max\_pending\_lw\_transactions | 10000 |
| hinted\_handoff\_enabled | hinted\_handoff\_enabled | TRUE |
| hints\_flush\_period\_in\_ms | hints\_flush\_period\_in\_ms | 10000 |
| enable\_user\_defined\_functions | enable\_user\_defined\_functions | FALSE |
| hinted\_handoff\_throttle\_in\_kb | hinted\_handoff\_throttle\_in\_kb | 10240 |
| max\_hint\_window\_in\_ms | max\_hint\_window\_in\_ms | 10800000 |
| otc\_coalescing\_strategy | otc\_coalescing\_strategy | DISABLED |
| user\_defined\_function\_warn\_heap\_mb | user\_defined\_function\_warn\_heap\_mb | 200 |
| auto\_snapshot | auto\_snapshot | TRUE |
| cdc\_raw\_directory | cdc\_raw\_directory | /data/cdc\_raw |
| range\_request\_timeout\_in\_ms | range\_request\_timeout\_in\_ms | 10000 |
| user\_function\_timeout\_policy | user\_function\_timeout\_policy | die |
| stream\_throughput\_outbound\_megabits\_per\_sec | stream\_throughput\_outbound\_megabits\_per\_sec | 200 |
| commitlog\_directory | commitlog\_directory | /commitlog |
| sstable\_preemptive\_open\_interval\_in\_mb | sstable\_preemptive\_open\_interval\_in\_mb | 50 |
| seed\_provider | seed\_provider |  |
| - class\_name | org.apache.cassandra.locator.SimpleSeedProvider |
| parameters |  |
| - seeds | 10.64.101.203, 10.64.161.205, 10.64.159.202, 10.64.102.205, 10.64.158.203,10.64.160.201, 10.64.101.201, 10.64.100.210, 10.64.160.202, 10.64.161.201, 10.64.159.203,10.64.100.207, 10.64.160.200, 10.64.158.205, 10.64.100.208, 10.64.159.201, 10.64.158.201,10.64.161.203, 10.64.102.203, 10.64.99.205, 10.64.99.203, 10.64.99.201, 10.64.101.200,10.64.102.201 |
| dynamic\_snitch\_update\_interval\_in\_ms | dynamic\_snitch\_update\_interval\_in\_ms | 100 |
| trickle\_fsync\_interval\_in\_kb | trickle\_fsync\_interval\_in\_kb | 10240 |
| commitlog\_sync\_period\_in\_ms | commitlog\_sync\_period\_in\_ms | 10000 |
| cdc\_enabled | cdc\_enabled | FALSE |
| max\_hints\_file\_size\_in\_mb | max\_hints\_file\_size\_in\_mb | 128 |
| counter\_write\_request\_timeout\_in\_ms | counter\_write\_request\_timeout\_in\_ms | 5000 |
| zerocopy\_streaming\_enabled | zerocopy\_streaming\_enabled | TRUE |
| cluster\_name | cluster\_name | MTT |
| zerocopy\_max\_sstables | zerocopy\_max\_sstables | 256 |
| endpoint\_snitch | endpoint\_snitch | GossipingPropertyFileSnitch |
| cross\_dc\_rtt\_in\_ms | cross\_dc\_rtt\_in\_ms | 0 |
| streaming\_connections\_per\_host | streaming\_connections\_per\_host | 1 |
| hints\_directory | hints\_directory | /data/hints |
| dynamic\_snitch\_badness\_threshold | dynamic\_snitch\_badness\_threshold | 0,1 |
| concurrent\_lw\_transactions | concurrent\_lw\_transactions | 128 |
| native\_transport\_max\_concurrent\_connections\_per\_ip | native\_transport\_max\_concurrent\_connections\_per\_ip | -1 |
| user\_defined\_function\_fail\_heap\_mb | user\_defined\_function\_fail\_heap\_mb | 500 |
| permissions\_validity\_in\_ms | permissions\_validity\_in\_ms | 1200000 |
| roles\_validity\_in\_ms | roles\_validity\_in\_ms | 1200000 |
| cas\_contention\_timeout\_in\_ms | cas\_contention\_timeout\_in\_ms | 1000 |
| seed\_gossip\_probability | seed\_gossip\_probability | 1 |
| zerocopy\_max\_unused\_metadata\_in\_mb | zerocopy\_max\_unused\_metadata\_in\_mb | 200 |
| native\_transport\_max\_concurrent\_connections | native\_transport\_max\_concurrent\_connections | -1 |
| aggregated\_request\_timeout\_in\_ms | aggregated\_request\_timeout\_in\_ms | 120000 |

* Thông số File dse.yaml:

| **Dạng tham số** | **Tham số** | **Giá trị** |
| --- | --- | --- |
| spark\_cluster\_info\_options | spark\_cluster\_info\_options |  |
| enabled | false |
| system\_info\_encryption | system\_info\_encryption |  |
| enabled | false |
| authentication\_options | authentication\_options |  |
| enabled | true |
| default\_scheme | internal |
| other\_schemes | [] |
| scheme\_permissions | false |
| allow\_digest\_with\_kerberos | true |
| plain\_text\_without\_ssl | warn |
| transitional\_mode | disabled |
| spark\_security\_enabled | spark\_security\_enabled | false |
| config\_encryption\_active | config\_encryption\_active | false |
| histogram\_data\_options | histogram\_data\_options |  |
| enabled | false |
| performance\_queue\_capacity | performance\_queue\_capacity | 32000 |
| spark\_security\_encryption\_enabled | spark\_security\_encryption\_enabled | false |
| spark\_process\_runner | spark\_process\_runner |  |
| runner\_type | default |
| run\_as\_runner\_options |  |
| user\_slots |  |
| - slot1 | - slot1 |
| - slot2 | - slot2 |
| solr\_resource\_upload\_limit\_mb | solr\_resource\_upload\_limit\_mb | 10 |
| resource\_level\_latency\_tracking\_options | resource\_level\_latency\_tracking\_options |  |
| enabled | false |
| spark\_application\_info\_options | spark\_application\_info\_options |  |
| enabled | false |
| driver |  |
| sink | false |
| connectorSource | false |
| jvmSource | false |
| stateSource | false |
| executor |  |
| sink | false |
| connectorSource | false |
| jvmSource | false |
| graph | graph |  |
| max\_query\_params | 16 |
| adjacency\_cache\_size\_in\_mb | 128 |
| system\_evaluation\_timeout\_in\_seconds | 180 |
| index\_cache\_size\_in\_mb | 128 |
| analytic\_evaluation\_timeout\_in\_minutes | 10080 |
| schema\_agreement\_timeout\_in\_ms | 10000 |
| realtime\_evaluation\_timeout\_in\_seconds | 30 |
| gremlin\_server |  |
| port | 8182 |
| threadPoolWorker | 2 |
| scriptEngines |  |
| gremlin-groovy |  |
| config |  |
| sandbox\_enabled | false |
| kerberos\_options | kerberos\_options |  |
| keytab | /etc/dse/conf/dse.keytab |
| service\_principal | dse/\_HOST@REALM |
| http\_principal | HTTP/\_HOST@REALM |
| qop | auth |
| user\_level\_latency\_tracking\_options | user\_level\_latency\_tracking\_options |  |
| enabled | false |
| dsefs\_options | dsefs\_options |  |
| work\_dir | /data/dsefs\_dr |
| public\_port | 5598 |
| query\_cache\_size | 2048 |
| compression\_frame\_max\_size | 1048576 |
| gossip\_options |  |
| round\_delay\_ms | 2000 |
| startup\_delay\_ms | 5000 |
| shutdown\_delay\_ms | 10000 |
| service\_startup\_timeout\_ms | 30000 |
| enabled | true |
| rest\_options |  |
| request\_timeout\_ms | 330000 |
| connection\_open\_timeout\_ms | 55000 |
| client\_close\_timeout\_ms | 60000 |
| server\_request\_timeout\_ms | 300000 |
| idle\_connection\_timeout\_ms | 0 |
| private\_port | 5599 |
| keyspace\_name | dsefs\_dr |
| transaction\_options |  |
| transaction\_timeout\_ms | 60000 |
| conflict\_retry\_delay\_ms | 10 |
| conflict\_retry\_count | 40 |
| execution\_retry\_delay\_ms | 1000 |
| execution\_retry\_count | 3 |
| server\_close\_timeout\_ms | 2147483647 |
| data\_directories |  |
| - dir | /data/dsefs\_dr/data |
| min\_free\_space | 268435456 |
| storage\_weight | 1 |
| block\_allocator\_options |  |
| overflow\_margin\_mb | 1024 |
| overflow\_factor | 1.05 |
| service\_close\_timeout\_ms | 600000 |
| internode\_authentication |  |
| enabled | true |
| algorithm | HmacSHA256 |
| query\_cache\_expire\_after\_ms | 2000 |
| solr\_request\_handler\_metrics\_options | solr\_request\_handler\_metrics\_options |  |
| enabled | false |
| spark\_daemon\_readiness\_assertion\_interval | spark\_daemon\_readiness\_assertion\_interval | 1000 |
| spark\_shared\_secret\_bit\_length | spark\_shared\_secret\_bit\_length | 256 |
| cql\_solr\_query\_paging | cql\_solr\_query\_paging | off |
| internode\_messaging\_options | internode\_messaging\_options |  |
| client\_max\_connections | 200 |
| port | 8609 |
| performance\_max\_threads | performance\_max\_threads | 32 |
| insights\_options | insights\_options |  |
| log\_dir | /u01/log/dse/insights |
| data\_dir | /data/insights |
| async\_bootstrap\_reindex | async\_bootstrap\_reindex | false |
| alwayson\_sql\_options | alwayson\_sql\_options |  |
| reserve\_port\_wait\_time\_ms | 100 |
| web\_ui\_port | 9077 |
| enabled | true |
| runner\_max\_errors | 10 |
| alwayson\_sql\_status\_check\_wait\_time\_ms | 500 |
| workpool | alwayson\_sql |
| log\_dsefs\_dir | /spark/log/alwayson\_sql |
| auth\_user | alwayson\_sql |
| thrift\_port | 10000 |
| enable\_health\_based\_routing | enable\_health\_based\_routing | true |
| lease\_metrics\_options | lease\_metrics\_options |  |
| enabled | false |
| ram\_buffer\_offheap\_space\_in\_mb | ram\_buffer\_offheap\_space\_in\_mb | 1024 |
| back\_pressure\_threshold\_per\_core | back\_pressure\_threshold\_per\_core | 1024 |
| node\_health\_options | node\_health\_options |  |
| refresh\_rate\_ms | 60000 |
| uptime\_ramp\_up\_period\_seconds | 10800 |
| dropped\_mutation\_window\_minutes | 30 |
| solr\_encryption\_options | solr\_encryption\_options |  |
| decryption\_cache\_offheap\_allocation | true |
| decryption\_cache\_size\_in\_mb | 256 |
| solr\_latency\_snapshot\_options | solr\_latency\_snapshot\_options |  |
| enabled | false |
| db\_summary\_stats\_options | db\_summary\_stats\_options |  |
| enabled | false |
| enable\_index\_disk\_failure\_policy | enable\_index\_disk\_failure\_policy | false |
| resource\_manager\_options | resource\_manager\_options |  |
| worker\_options |  |
| cores\_total | '0.7' |
| memory\_total | '0.6' |
| workpools | [] |
| solr\_cache\_stats\_options | solr\_cache\_stats\_options |  |
| enabled | false |
| cluster\_summary\_stats\_options | cluster\_summary\_stats\_options |  |
| enabled | false |
| max\_memory\_to\_lock\_mb | max\_memory\_to\_lock\_mb | 10240 |
| solr\_slow\_sub\_query\_log\_options | solr\_slow\_sub\_query\_log\_options |  |
| enabled | false |
| system\_key\_directory | system\_key\_directory | /u01/app/dse/conf |
| solr\_index\_stats\_options | solr\_index\_stats\_options |  |
| enabled | false |
| audit\_logging\_options | audit\_logging\_options |  |
| logger | SLF4JAuditWriter |
| excluded\_categories | QUERY |
| enabled | true |
| included\_keyspaces | ks\_dangky, ks\_danhmuc, ks\_hddt\_system, ks\_hoadon, ks\_hosogoc, ks\_ht\_tacnghiep, ks\_kad, ks\_luutam, ks\_tintuc, ks\_tdt\_system |
|  |  |
| retention\_time | 0 |
| render\_cql\_literals | true |
| cassandra\_audit\_writer\_options |  |
| mode | sync |
| queue\_size | 30000 |
| write\_consistency | QUORUM |
| dropped\_event\_log | /var/log/cassandra/dropped\_audit\_events.log |
| day\_partition\_millis | 3600000 |
| cql\_slow\_log\_options | cql\_slow\_log\_options |  |
| enabled | true |
| threshold | 200 |
| minimum\_samples | 100 |
| ttl\_seconds | 259200 |
| skip\_writing\_to\_db | true |
| num\_slowest\_queries | 5 |
| cql\_solr\_query\_row\_timeout | cql\_solr\_query\_row\_timeout | 10000 |
| solr\_update\_handler\_metrics\_options | solr\_update\_handler\_metrics\_options |  |
| enabled | false |
| ram\_buffer\_heap\_space\_in\_mb | ram\_buffer\_heap\_space\_in\_mb | 1024 |
| cql\_system\_info\_options | cql\_system\_info\_options |  |
| enabled | false |
| advanced\_replication\_options | advanced\_replication\_options |  |
| enabled | false |
| solr\_field\_cache\_enabled | solr\_field\_cache\_enabled | false |
| spark\_ui\_options | spark\_ui\_options |  |
| encryption | inherit |
| encryption\_options |  |
| enabled | false |
| flush\_max\_time\_per\_core | flush\_max\_time\_per\_core | 5 |
| max\_memory\_to\_lock\_fraction | max\_memory\_to\_lock\_fraction | 0.2 |
| performance\_core\_threads | performance\_core\_threads | 4 |
| authorization\_options | authorization\_options |  |
| enabled | true |
| transitional\_mode | disabled |
| allow\_row\_level\_security | false |
| shard\_transport\_options | shard\_transport\_options |  |
|  | user\_memberof\_attribute | memberof |
| ssl\_protocol | TLS |
| group\_search\_type | directory\_search |
| search\_password | ' |
| all\_parent\_groups\_memberof\_attribute | isMemberOf |
| credentials\_validity\_in\_ms | 0 |
| truststore\_path | '' |
| groups\_update\_interval\_in\_ms | 0 |
| groups\_validity\_in\_ms | 0 |
| search\_validity\_in\_seconds | 0 |
| user\_search\_base | '' |
| user\_search\_filter | (uid={0}) |
| server\_host | '' |
| hostname\_verification | false |
| group\_name\_attribute | cn |
| server\_port | 389 |
| use\_ssl | false |
| truststore\_type | jks |
| connection\_pool |  |
| max\_active | 8 |
| max\_idle | 8 |
| search\_dn | '' |
| extra\_group\_search\_bases | [] |
| group\_search\_filter | (uniquemember={0}) |
| dns\_service\_discovery |  |
| lookup\_timeout\_ms | 5000 |
| retention\_duration\_ms | 600000 |
| polling\_interval\_ms | 0 |
| use\_tls | false |
| extra\_user\_search\_bases | [] |
| ttl\_index\_rebuild\_options | ttl\_index\_rebuild\_options |  |
| fixed\_rate\_period | 300 |
| initial\_delay | 20 |
| max\_docs\_per\_batch | 4096 |
| thread\_pool\_size | 1 |
| load\_max\_time\_per\_core | load\_max\_time\_per\_core | 5 |
| graph\_events | graph\_events |  |
| ttl\_seconds | 600 |

* Thông số File dse.conf

spark {

job-number-cpus = 4

jobserver {

port = 8090

}

context-settings {

num-cpu-cores = 2

memory-per-node = 512m

passthrough {

}

}

}

deploy {

manager-start-cmd = "dse spark-jobserver context-per-jvm-managed-start"

}

##### Thông số Datacenter

| **THAM SỐ DR\_ANA** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| Tên DC | DR\_Ana |  |
| Số lượng Node bổ sung | 4 |  |
| Workload | Analytics + Search |  |

##### Thông số Logical Rack

Logical Rack của DR\_Ana được thiết kế dựa trên những nguyên tắc:

* Số lượng rack vật lý: 01 tủ rack.
* Một logical rack của một datacenter không được nằm trên cùng một rack vật lý.
* Yếu tố nhân bản dữ liệu (Replication Factor): RF=2.
* Số node trong một datacenter phân bổ đều trên các logical rack.
* Tải trên hệ thống khi một logical rack đưa vào chế độ bảo trì.
* Dễ mở rộng hệ thống trong tương lai.

Từ những nguyên tắc trên, nhà thầu đưa ra quy hoạch logical rack và phân bổ các node của mỗi datacenter trên rack đảm bảo tối ưu nhất có thể như sau:

* Datacenter DR\_Ana:
* Số lượng node: 4
* Logical rack: 02
* Số lượng nodes trên logical rack dr\_ana1: 2
* Số lượng nodes trên logical rack dr\_ana2: 2
* Thông tin được hiển thị chi tiết theo bảng sau:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **TT** | **DC** | **Tham số** | **Physical Rack** | | **Tổng** |
| **Rack D11** | |
| 1 | DR\_Ana 4 node (RF=2) | Chassis | 1 | | 1 |
| Nodes | 4 | | 4 |
| Logical Rack ID | dr\_ana1 | dr\_ana2 |  |

##### Thông số các Node CSDL Ana

Thông số cấu hình từng node CSDL Ana như sau:

| **CẤU HÌNH TỪNG NODE ANA** | | |
| --- | --- | --- |
| **Tham số** | **Giá trị** | **Chú thích** |
| CPU | 2 x 12 Core |  |
| RAM | 128 GB |  |
| Disk | 04 x 960GB (SSD) |  |
| Network | 04 x 10 Gigabit (Gbps) Ethernet port | Bonding (802.3ad) |
| OS | RHEL 8.10 | Red Hat Enterprise Linux 8.10 |
| Đường dẫn file data | /data/data | Dữ liệu SSTables |
| Đường dẫn commit log | /commitlog | Dữ liệu commit log |
| Đường dẫn file log | /u01/log/dse/cassandra/ | Lưu log của DSE |
| Khả năng lưu trữ | ~ 2.6TiB |  |
| DNS | 10.64.88.11 |  |
| 10.64.88.12 |
| NTP | 10.64.68.26 |  |

##### Keyspace & Replication

###### Danh sách các keyspace cho DR\_Ana

| **STT** | **Keyspace** | **Replicate Factor (DC\_Ana)** | **Replication Strategy** |
| --- | --- | --- | --- |
| 1 | ks\_hoadon | 2 | NetworkTopologyStrategy |
| 3 | ks\_kad | 2 | NetworkTopologyStrategy |
| 5 | ks\_luutam | 2 | NetworkTopologyStrategy |
| 6 | ks\_danhmuc | 2 | NetworkTopologyStrategy |
| 7 | ks\_tdt\_system | 2 | NetworkTopologyStrategy |
| 8 | ks\_hddt\_system | 2 | NetworkTopologyStrategy |
| 9 | ks\_baocao | 2 | NetworkTopologyStrategy |
| 10 | ks\_dangky | 2 | NetworkTopologyStrategy |
| 11 | dse\_leases | 3 | NetworkTopologyStrategy |
| 12 | dse\_security | 3 | NetworkTopologyStrategy |
| 13 | dsefs | 3 | NetworkTopologyStrategy |
| 14 | dse\_audit | 1 | NetworkTopologyStrategy |
| 15 | dse\_analytics | 3 | NetworkTopologyStrategy |
| 16 | dse\_perf | 2 | NetworkTopologyStrategy |
| 17 | system\_auth | 3 | NetworkTopologyStrategy |
| 18 | system\_distributed | 2 | NetworkTopologyStrategy |
| 19 | spark\_jobserver | 2 | NetworkTopologyStrategy |
| 20 | HiveMetaStore | 3 | NetworkTopologyStrategy |
| 21 | OpsCenter | 2 | NetworkTopologyStrategy |
| 22 | monitor | 2 | NetworkTopologyStrategy |
| 23 | temp | 2 | NetworkTopologyStrategy |

###### Lựa chọn Replicate Factor

Cassandra lưu trữ các bản sao trên nhiều node để đảm bảo độ tin cậy và khả năng chịu lỗi. Chiến lược sao chép (Replication Strategy) xác định các node nơi đặt bản sao. Tổng số bản sao trên toàn bộ cluster được gọi là replication factor (RF). RF = 1 có nghĩa là chỉ có một bản sao của mỗi row trong cluster. Nếu node chứa row bị hỏng, row đó không thể được truy xuất. RF= 2 có nghĩa là hai bản sao của mỗi row, trong đó mỗi bản sao nằm trên một node khác nhau. Tất cả các bản sao đều quan trọng như nhau; không có primary hay master copy. Theo nguyên tắc chung, RF không được vượt quá số node trong cụm. Tuy nhiên, có thể tăng RF và sau đó thêm số node mong muốn sau.

Hai Replication Strategy có sẵn:

* SimpleStrategy: Chỉ sử dụng cho một trung tâm dữ liệu đơn và rack đơn.

A picture containing diagram

Description automatically generated

Các node kế tiếp hoặc các node trên ring ngay lập tức tuân theo gọi theo chiều kim đồng hồ đến nút điều phối được chọn làm bản sao.

* NetworkTopologyStrategy: Được khuyến khích cho hầu hết các tình huống triển khai vì việc mở rộng sang nhiều DC khi cần mở rộng trong tương lai sẽ dễ dàng hơn nhiều.

Graphical user interface

Description automatically generated with medium confidence

Các node từ các rack riêng biệt trong mỗi DC được chọn làm bản sao. Người quản trị cần chỉ định hệ số RF cho mỗi DC trong môi trường có nhiều DC. Trong mỗi DC, các nút kế tiếp cho nút điều phối được đặt trên các rack riêng biệt được chọn.

Đối với DR\_Ana, hệ số Replicate Factor được chọn là 2.

###### Thông số RF cho Keyspace

Cassandra lưu trữ các bản replicas trên nhiều node khác nhau theo chiến lược NetworkTopologyStrategy và tham số Replication Factor (RF) của từng keyspace.

Số lượng RF cho mỗi keyspace trong DR\_Ana được phân bố theo bảng sau:

| **STT** | **Keyspace** | **Replicate Factor (DC\_Ana)** | **Replication Strategy** |
| --- | --- | --- | --- |
| 1 | ks\_hoadon | 2 | NetworkTopologyStrategy |
| 3 | ks\_kad | 2 | NetworkTopologyStrategy |
| 5 | ks\_luutam | 2 | NetworkTopologyStrategy |
| 6 | ks\_danhmuc | 2 | NetworkTopologyStrategy |
| 7 | ks\_tdt\_system | 2 | NetworkTopologyStrategy |
| 8 | ks\_hddt\_system | 2 | NetworkTopologyStrategy |
| 9 | ks\_baocao | 2 | NetworkTopologyStrategy |
| 10 | ks\_dangky | 2 | NetworkTopologyStrategy |
| 14 | dse\_leases | 3 | NetworkTopologyStrategy |
| 15 | dse\_security | 3 | NetworkTopologyStrategy |
| 16 | dsefs | 3 | NetworkTopologyStrategy |
| 20 | dse\_audit | 1 | NetworkTopologyStrategy |
| 21 | dse\_analytics | 3 | NetworkTopologyStrategy |
| 22 | dse\_perf | 2 | NetworkTopologyStrategy |
| 23 | system\_auth | 3 | NetworkTopologyStrategy |
| 24 | system\_schema |  |  |
| 25 | system\_distributed | 2 | NetworkTopologyStrategy |
| 30 | spark\_jobserver | 2 | NetworkTopologyStrategy |
| 31 | HiveMetaStore | 3 | NetworkTopologyStrategy |
| 32 | OpsCenter | 2 | NetworkTopologyStrategy |
| 33 | monitor | 2 | NetworkTopologyStrategy |
| 34 | temp | 2 | NetworkTopologyStrategy |

#### Thiết kế an toàn bảo mật cho máy chủ CSDL Ana tại TTDL Dự phòng

##### Xác thực trên máy chủ

* Xác thực trên máy chủ để xác thực người dùng khi truy cập, quản lý và sử dụng máy chủ. Các máy chủ sử dụng tài khoản local để quản lý, giám sát, vận hành. Cụ thể:
* Quyền Administrator: có toàn quyền trên thiết bị.
* Quyền Operator: có quyền quản trị thiết bị.
* Quyền Monitor: chỉ có quyền giám sát thiết bị.
* Thay đổi các tài khoản mặc định trên hệ thống hoặc vô hiệu hóa (nếu không sử dụng): Máy chủ chỉ enable các tài khoản quản trị hệ thống, quản trị ứng dụng/csdl, giám sát thiết bị. Các tài khoản khách, tài khoản mặc định bị disabled.
* Yêu cầu với mật khẩu trên máy chủ:
* Thay đổi mật khẩu mặc định: mật khẩu được thay đổi theo các quy tắc an toàn bảo mật và bàn giao sau khi cài đặt.
* Quy tắc đặt mật khẩu về số ký tự, loại ký tự: Có tối thiểu 8 ký tự, gồm chữ cái viết hoa (A - Z), chữ cái viết thường (a - z), chữ số (0 – 9) và ký tự đặc biệt.
* Thời gian yêu cầu thay đổi mật khẩu: 90 ngày (không bắt buộc đối với tài khoản dùng để xác thực kết nối giữa máy chủ với các hệ thống khác).
* Chi tiết cấu hình yêu cầu với mật khẩu trên máy chủ như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Thời gian hiệu lực tối đa của mật khẩu: xác định số ngày tối đa mà mật khẩu hợp lệ. | Cấu hình trong /etc/login.defs PASS\_MAX\_DAYS=90 |
| 2 | Độ dài tối thiểu của mật khẩu | Cấu hình trong /etc/security/pwquality.conf minlen=8 |
| 3 | Số loại ký tự khác nhau trong mật khẩu: xác định số loại ký tự (chữ, số, ký tự đặc biệt...) trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  minclass=4 |
| 4 | Số ký tự chữ cái viết thường tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  lcredit=-1 |
| 5 | Số ký tự chữ cái viết hoa tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  ucredit=-1 |
| 6 | Số chữ số tối thiểu trong mật khẩu | Cấu hình trong /etc/security/pwquality.conf  dcredit=-1 |
| 7 | Số ký tự đặc biệt tối thiểu trong mật khẩu. | Cấu hình trong /etc/security/pwquality.conf  ocredit=-1 |

* Các chính sách GPO liên quan chứng thực tài khoản như sau:

| **STT** | **Mô tả yêu cầu** | **Cấu hình chi tiết** |
| --- | --- | --- |
| 1 | Số lần đăng nhập sai trong khoảng thời gian nhất định với một tài khoản nhất định: 5 lần | Cấu hình trong /etc/security/faillock.conf deny=5 |
| 2 | Mở khóa tài khoản nếu tài khoản đó đăng nhập sai vượt quá 5 lần: 300 giây | Cấu hình trong /etc/security/login.cfg  unlock\_time=300 |
| 3 | Thiết lập thời gian ngắt kết nối khi không sử dụng: 300 giây | Cấu hình trong /etc/profile.d/tct\_sessiontimeout.sh readonly TIMEOUT=300 |

##### Kiểm soát truy cập

* Sử dụng các kết nối mạng an toàn khi truy cập, quản trị máy chủ từ xa.
* Thiết lập giới hạn thời gian chờ: 10 phút kể từ khi người dùng không có thao tác (idle), tài khoản sẽ tự động logout.
* Thay đổi cổng quản trị mặc định của máy chủ: Các cổng quản trị mặc định được thay đổi hoặc khóa cổng mặc định (Telnet) ngay sau khi hoàn thành cài đặt.
* Các thiết bị chỉ được truy cập từ các máy chủ terminal hoặc CA PAM.

##### Nhật ký hệ thống (logs)

* Thiết bị được cấu hình ghi nhật ký hệ thống (log) bao gồm những thông tin sau:
* Thông tin đăng nhập vào máy chủ.
* Lỗi phát sinh trong quá trình hoạt động.
* Thông tin thay đổi cấu hình máy chủ.
* Giới hạn đủ dung lượng lưu trữ nhật ký hệ thống: Mỗi máy chủ được cấu hình log với dung lượng không quá 500Mb hoặc thời gian lưu trữ không quá 6 tháng.
* Lưu trữ tập trung nhật ký hệ thống tới hệ thống xử lý log tập trung.
* Thông tin hệ thống logs như sau:
* Hệ thống Logs Splunk:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.158 | 9997 |
| 10.64.212.159 | 9997 |
| 10.64.212.213 | 9997 |

* Hệ thống Logs ELK cho máy chủ APP:

| **IP address** | **Port** |
| --- | --- |
| 10.64.212.215 | 5044 |

* Thông tin hệ thống SOC/SIEM sẽ được tích hợp:

| **IP address** | **Port** |
| --- | --- |
| 10.64.166.173 | 514 |

##### Phòng chống xâm nhập và các yêu cầu khác

* Vô hiệu hóa các giao thức mạng không an toàn, các dịch vụ hệ thống không sử dụng: SMB v1 (nếu có), WDigest Authentication (nếu có), Allow Basic authentication (nếu có).
* Phòng chống phần mềm độc hại: Trend Micro Deep Security

| **IP address** | **Port** |
| --- | --- |
| 10.64.213.67 | 4119  4120 |

* Đồng bộ thời gian giữa máy chủ với máy chủ NTP Server.
* Thông số các máy chủ NTP Server của TCT như sau:

|  |  |
| --- | --- |
| NTP Server | 10.64.68.26 |