# Disaster Recovery Standard Operating Procedures

# Table of Contents

|  |  |  |  |
| --- | --- | --- | --- |
| **Topic No.** | **Name of Topic** | | **Page** |
| **1** | **Introduction -----------------------------------------------------------------------------------------------** | | **3** |
| **2** | **Response Teams ------------------------------------------------------------------------------------------** | | **4** |
| **3** | **Steps before initiating the DR Plan-------------------------------------------------------------------** | | **5** |
| **4** | **DR Plans------------------------------------------------------------------------------------------------------** | | **6** |
| **5** | **DR Plan A----------------------------------------------------------------------------------------------------** | | **7**  **7**  **8** |
| **5.1** | **Considerations before executing this plan-------------------------------------------------** |
| **5.2** | **Steps to execute the DR Plan A:** **--------------------------------------------------------------** |
| **6** | **DR Plan B-----------------------------------------------------------------------------------------------------** | | **11**  **11**  **14** |
| **6.1** | **Considerations before executing this plan-------------------------------------------------** |
| **6.2** | **Steps to execute the DR Plan B:** **--------------------------------------------------------------** |
| **7** | **DR Plan C-----------------------------------------------------------------------------------------------------** | | **18**  **18**  **19**  **23** |
| **7.1** | **Considerations before executing this plan-------------------------------------------------** |
| **7.2** | **Backup Strategy used for on-premise backup--------------------------------------------** |
| **7.3** | **Steps to execute the DR Plan C:** **--------------------------------------------------------------** |
| **8** | **Project Teamlocus DR Plans----------------------------------------------------------------------------** | | **24** |
|  | **8.1** | **Architectural overview of project Teamlocus Disaster Recovery--------------------** | **24** |
|  | **8.2** | **Steps to execute the DR Plan A:** **--------------------------------------------------------------** | **26** |
|  | **8.3** | **Steps to execute the DR Plan B:** **--------------------------------------------------------------** | **26** |
|  | **8.4** | **Steps to execute the DR Plan C:** **--------------------------------------------------------------** | **27** |
| **9** | **Project Pandoarch DR Plans----------------------------------------------------------------------------** | | **28** |
|  | **8.1** | **Architectural overview of project Pandoarch Disaster Recovery--------------------** | **28** |
|  | **8.2** | **Steps to execute the DR Plan A:** **--------------------------------------------------------------** | **29** |
|  | **8.3** | **Steps to execute the DR Plan B:** **--------------------------------------------------------------** | **29** |
|  | **8.4** | **Steps to execute the DR Plan C:** **--------------------------------------------------------------** | **30** |
| **10** | **Project APT DR Plans-------------------------------------------------------------------------------------** | | **31** |
|  | **10.1** | **Architectural overview of project APT Disaster Recovery-----------------------------** | **31** |
|  | **10.2** | **Steps to execute the DR Plan A:** **--------------------------------------------------------------** | **33** |
|  | **10.3** | **Steps to execute the DR Plan B:** **--------------------------------------------------------------** | **33** |
|  | **10.4** | **Steps to execute the DR Plan C:** **--------------------------------------------------------------** | **33** |

# Introduction

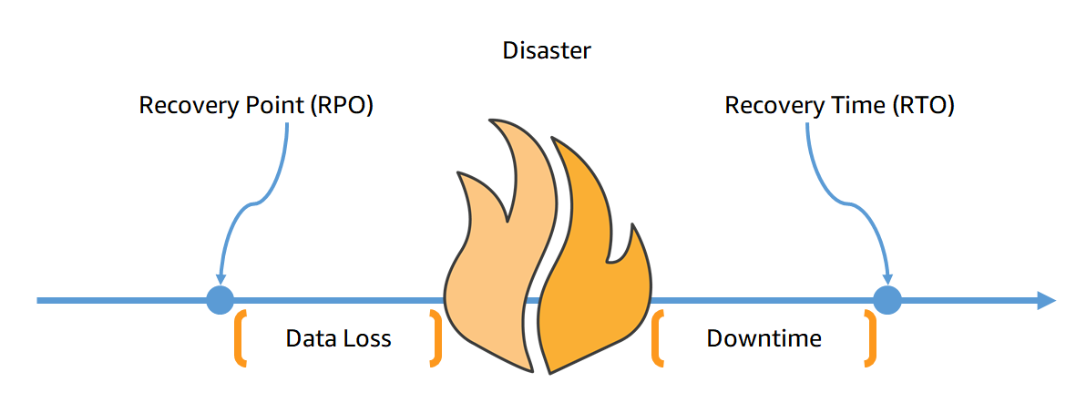


Figure 1: RPO and RTO in Disaster Recovery.

It is very important to set the backup strategies so that in case of any disaster with the infrastructure we can easily recover the data and reduce downtime depending upon the DR strategies.

RPO and RTO measuredly depend upon the DR policies that are used in the organization and we can implement it as per the use case and the severity of the project. The backup frequency defines the data loss that occurs due to disaster and we can decrease it by taking more frequent backups but it also depends upon the RPO needed to meet the company needs. If you need lesser RPO then you have to increase the frequency of the backup.

RTO will depend on the DR strategy and the severity of disaster which occurred. If the severity of disaster is more means we need to recovery everything that get lost in the event of disaster and in this case we need very strong DR strategy and only one DR strategy is not sufficient in all types of disaster incidents. We can reduce the downtime by implementing more mature and fully managed AWS services which will get our infrastructure and project live with very minimal efforts and less downtime. Mostly, decreasing RTO comes with increased cost and smart infrastructure automation which we need to use after the disaster.

So, we have to reduce the RPO for the servers where we have the databases so that we can reduce the data loss in case of disaster and we can keep RPO little larger for the application or less frequently modified servers. In all the cases we must reduce RTO as small as possible so that we end up with minimal downtime and fast recovery from the disaster. We have most of the workloads on AWS cloud so; we can take benefit of AWS services to carry out automated backups and recovery procedures in the disaster incidents. We are implementing those DR strategies based upon projects, severity, and type of servers and most importantly to follow the correct procedure in event of disaster.

# Response Teams

|  |  |  |
| --- | --- | --- |
| **Name of the Team** | **Team Member** | **Email** |
| **Cloud Team** | Amit Amin | amitra@deepfoods.com |
| Aniket Sanghoi | aniketjs@teamlocus.net |
| Ritesh Nadgive | riteshsn@teamlocus.net |
| Usama Mashayak | usamam@teamlocus.net |
| **Linux Team** | Nayan Gohel | nayanbg@teamlocus.net |
| Ankit Bakraniya | ankitbb@teamlocus.net |
| **Support Team** | Darpan Danani | darpannd@tasktower.net |
| Bhargav Hingu | bhargavmh@teamlocus.net |
| **Project Team** | Respected Project Personnel should be involved | NA |
| **Approval Authorities** | Archit Amin  Brijesh Patel | archie@deepfoods.com  brijeshnp@tasktower.com |

# Steps before initiating the DR Plan

* If you got any disaster incident on AWS infrastructure then you first need to contact the approval person and let him know the severity of the incident.
* You need to inform the associated project person from the tags attached to the resources and keep that person in the loop so that in case of recovery you might not wait for the concern person to be available.
* After deciding mutually the severity of the incident you can go ahead by taking approval from the approval person before executing any of the disaster recovery plan stated in this document.
* All the plans are concerned with the severity type and depend upon the scenario so please choose carefully Plan before executing any plan.
* You should communicate with the teams described in Response Teams before executing DR Plan.

# DR Plans

For the Projects we have 3 different DR solutions namely DR-Plan-A, DR-Plan-B, DR-Plan-C depending upon disaster severity.

Table 1: DR Plan Severity Cases and respective RPO and RTO

|  |  |  |  |
| --- | --- | --- | --- |
| **DR Plans** | **Severity case** | **RPO (Data Loss)** | **RTO (Downtime)** |
| DR-Plan-A | Ransomware, Disk Failure | < 15 Minutes | 10 Minutes |
| DR-Plan-B | Server status failed, OS failure, AZ down | < 1 Day | 10 Minutes |
| DR-Plan-C | Overall AWS Infrastructure is down | < 1 Day | < 2 Hours (May vary) |

**DR-Plan-A:**

In case of Ransomware attack on particular database server you can execute the DR-Plan-A which has the backup frequency of 15min via lambda function as snapshot restore. You can create the volume and attach it to the affected server back and run ransomware check.

If there is disk failure on the server and you are getting status check failures then you can execute the plan A.

**DR-Plan-B:**

If we have a condition where server goes into OS failure status check or OS level corruption occurs then you can execute DR-Plan-B. You can launch the server from the AMI which was created from the AWS backup service with frequency of 1 Day so please consider that you will have the RPO of 1Day in this DR plan.

**DR-Plan-C:**

This is the worst case scenario where our overall AWS infrastructure is down and we don’t have access to any AWS resources then we can execute this DR plan. The difference in this plan is that we have backup of databases and we can recover them either on-premise or AWS by using AWS datasync service in other way. RTO may vary with the severity of disaster and the other factors but we assume the RTO to be 2 hours.

# DR Plan A

## 5.1 Consideration before executing this plan

1. This plan must be executed if you have issues as per the DR plan severity cases and by considering RPO and RTO requirements. (For more information please ref. Table: 1)
2. We need to create volume from the corresponding snapshot that was created by the lambda function every 15min.
3. You can refer the Server volume backup information table to use this plan.
4. You have option to recover the additional drives of the servers only.
5. If you want to recover the overall server then this plan will not be suitable for this use case so choose the plan wisely.
6. If you have only one volume attached to the instance and that is the root volume then you need to stop the instance and remove the old volume from the affected instance and then attach the newly created volume from the snapshot to the instance and then you need to start the instance which may leads to downtime which you must consider before executing this plan.

## 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details)

Identify the teamlocus server you need to execute DR Plan A verify if it falls under server information table for particular project. Please note down the volume drive letter and volume ID.

**Step 1:** Open the AWS Console and go to EC2 Service and from the left panel select snapshots tab. (Refer: Figure 2)

**Step 2:** Search with the volume ID in the search tab to get the snapshots related to the respective volume. (Refer: Figure 2)

**Step 3:** Arrange the snapshot in descending order by clicking on the started tab so that we get most recent snapshot at the top of list and we can have the option to select the snapshot of our choice. (Refer: Figure 2)

**Step 4:** Select the snapshot you need to restore as per the timestamp of snapshot and then click on Actions tab. (Refer: Figure 2)

**Step 5:** Select “Create volume from snapshot” options under the dropdown menu. (Refer: Figure 2)

**Step 6:** After step 5 a new window will open which is nothing but volume create wizard. Since volumes are availability zone specific you need to select the AZ exactly same as that of affected server so that we can attach the volume after creating it. (Refer: Figure 3)

**Step 7:** Add the appropriate tags as per the organizational tag policies. (Refer: Figure 3)

**Step 8:** After successfully verifying all the details click on Create volume button and volume will be created. And let the volume be available state. Please note down the volume ID of newly created volume for future use. (Refer: Figure 3)

**Step 9:** After the volume successful creation select the volume tab from the left panel of EC2 console. (Refer: Figure 4)

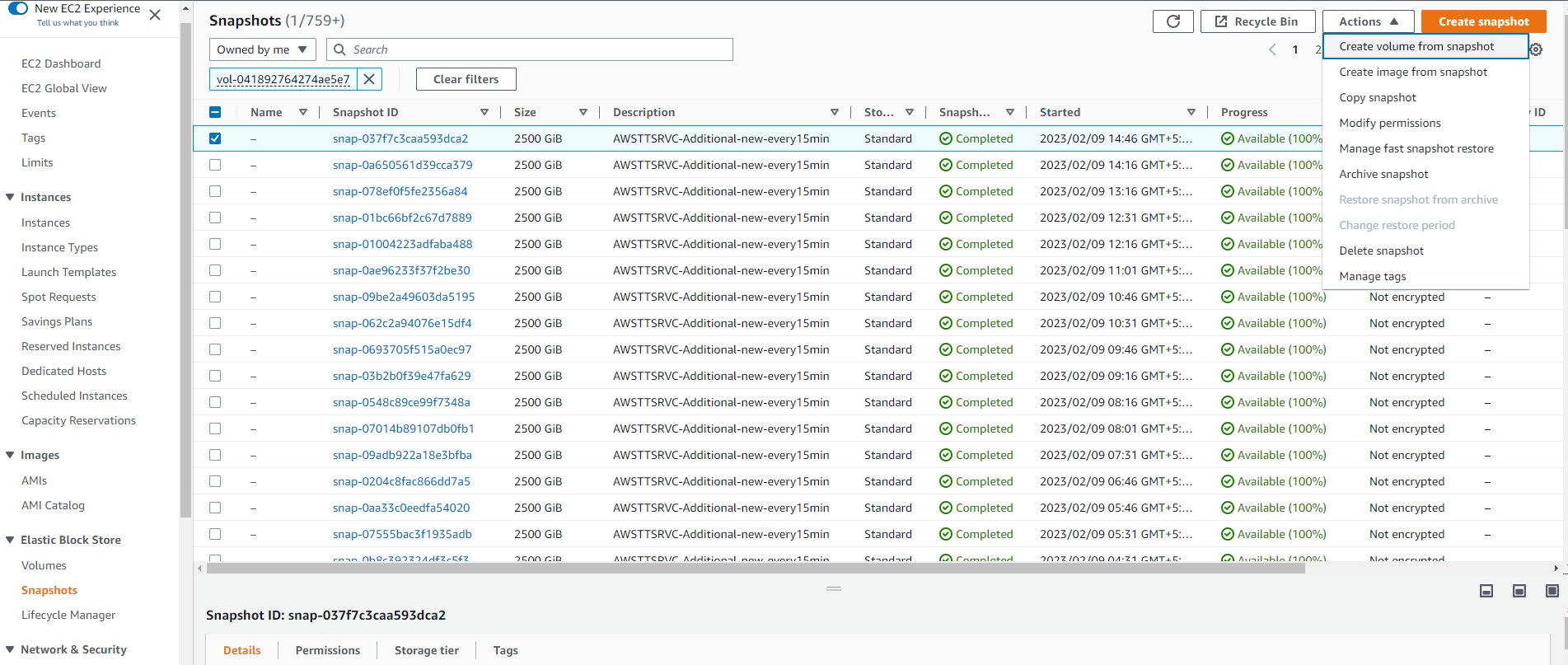
**Step 10:** Search the volume by placing volume ID in the search window and after selecting the volume go to the Actions tab and Select “Attach” option from the dropdown menu. (Refer: Figure 4)

**Step 11:** In the Volume attachment console please select the affected instance properly from the dropdown option, it’s better to put the instance ID of the instance to search exact instance. (Refer: Figure 5)

**Step 12:** Provide the “device name” carefully which has to be very similar to the earlier volume so that everything will work without breakdown. (Refer: Figure 5)

**Step 13:** After successfully entering all the details click on the attach volume button to attach volume to the instance. Also check if it’s available at the OS level. (Refer: Figure 5)

**4**



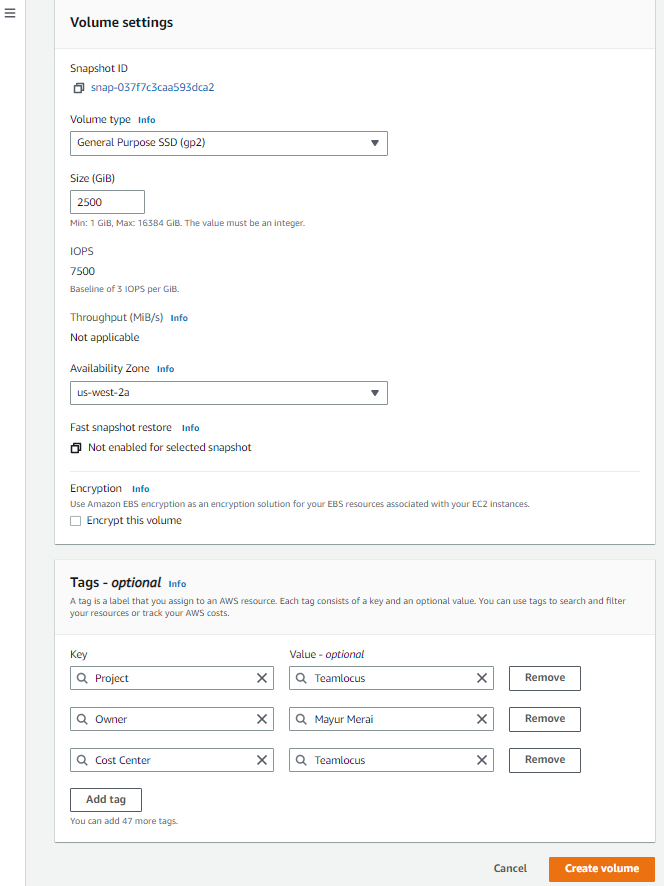
**1**

**2**

**3**

**5**

Figure 2: DR Plan A Steps (1-5).



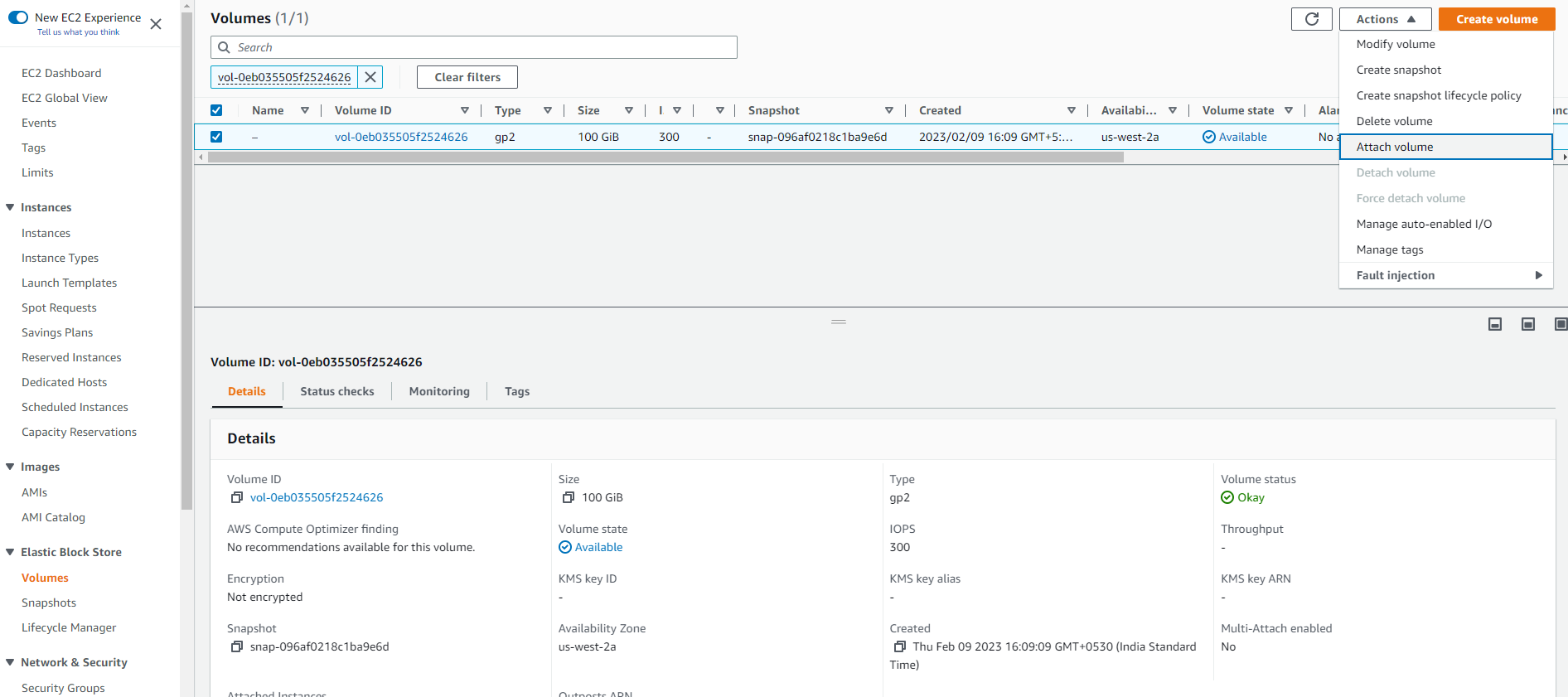
**6**

**7**

**8**

**8**

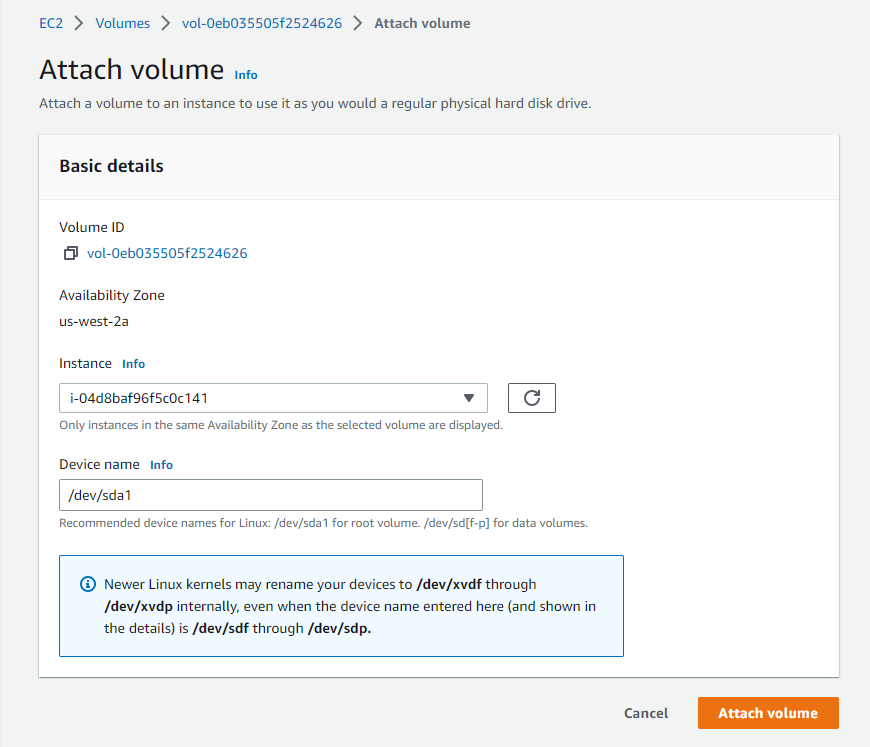
Figure 3: DR Plan A Steps (6-8).



**9**

**10**

Figure 4: DR Plan A Steps (9-10).



**13**

**12**

**11**

Figure 5: DR Plan A Steps (11-13).

# DR Plan B

## 6.1 Consideration before executing this plan:

1. Firstly, you should consider that RPO for this plan can have maximum value of 1 Day, so please choose this plan by keeping this consideration.
2. It makes use of AWS Backup service which takes backup as per the backup rule created and the selection of resources is based on the tags attached to the instances.
3. This is not the snapshot policy; it creates AMI which has all the volumes so while restoring it will create the new instance from the restore point.
4. We have different retentions as per the instance so please keep that in mind.
5. It is better to refer Table 2 for the backup retention and more details about the servers.
6. Before executing the Plan you must consider that you are going to launch new server so the details about the older server must be kept similar to avoid the unwanted breakdown of applications which are running.
7. If you want to retain private IP of the server then you have to terminate the older instance and give the same private IP and settings to the new instance only after successful terminating older instance.

Table 2: Servers Backup Details

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Instance ID** | **Name** | **Backup Frequency** | **Backup Retention** | **Contact** | **Email** | **Operating System** | **Owner** |
| i-0a75240e82f7c1303 | Twilio Brower Client | 1D | 15D | 9909333390 | parthnp@tasktower.net | Linux | Parth Patel |
| i-0c09875a5c8e80add | TT Drive | 1D | 15D | 8109650953 | vijaydwivedics@gmail.com | Linux | Vijay Dwivedi |
| i-08a1733634eb7e259 | TT Drive Onlyoffice | 1D | 15D | 8109650953 | vijaydwivedics@gmail.com | Linux | Vijay Dwivedi |
| i-0774ed3d2cf9c40d2 | TL AWSTLBatcher | 1D | 15D | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-09ea6f4b102a12a29 | TL Chat | 1D | 15D | 9909333390 | parthnp@tasktower.net | Linux | Parth Patel |
| i-0294fce4e841408af | Deepfoods Website | 1D | 15D | 8109650953 | vijaybd@tasktower.net | Bitnami | Vijay Dwivedi |
| i-0e859234c6f690731 | Batcher Lockholder Handpunch 2019 | 1D | 15D | 9979935263 | devendarbar@gmail.com | Windows | Devendra |
| i-755a54b2 | Voice1 Freepbx | 1D | 15D | 8306496543 | nayanbg@teamlocus.net | Linux | Nayan Gohel |
| i-0f00cfcfe97687605 | TL Email Beanstalk | 1D | 15D | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-0c7140b5f3dc14655 | Pandoarch Application 2019 | 1D | 15D | 9979935263 | devendarbar@gmail.com | Windows | Devendra |
| i-0bef605c3ecaff5c6 | Untangle New | 1D | 15D | 8866112655 | bharghavmh@teamlocus.net | Linux | Bhargav Hingu |
| i-0c31a5eef9ecdd667 | D AWSCTX42 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-04a9a8f3d6f500f32 | TL Chat File Server | 1D | 1M | 9909333390 | parthnp@tasktower.net | Linux | Parth Patel |
| i-0a8988c98b763c4f4 | D AWSCTX52 | 1D | 1M | 9925035568 | brijeshnp@tasktower.net | Windows | Brijesh Patel |
| i-0face7fbe1bb85c92 | D AWSCTX33 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-02fd7f0e7a86df1ad | D AWSCTX50 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0fcd4367017bacc12 | AWSCTX10 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-04d8baf96f5c0c141 | TL Chat DB Linux | 1D | 1M | 9909333390 | parthnp@tasktower.net | (not tagged) | Parth Patel |
| i-c6556ecb | AWSCTXSQL Exe | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0f72724db96cc1472 | AWSDC04 | 1D | 1M | 7405765456 | ankitrr@tasktower.com | Windows | Ankit Raval |
| i-004d99ebb978571bc | TT Chat Socket IO DB | 1D | 1M | 9909333390 | parthnp@tasktower.net | Windows | Parth Patel |
| i-06c3e7138ceaf7ef7 | ML Textract | 1D | 1M | 7405580347 | mayurjp@teamlocus.net | Linux | Mayur Patel |
| i-0b74ef5f82d277839 | D AWSCTX38 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-026d06fdf046a5aa6 | D AWSCTX39 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-2f654ff5 | Credit Card Server NJ | 1D | 1M | 7405765456 | ankitrr@tasktower.com | Windows | Ankit Raval |
| i-0680f99588266ea19 | D AWSCTX02 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0dad4ebe5ec777475 | D AWSCTX51 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-69d726b0 | IT-Autosnapshot Prashant | 1D | 1M | 7405765456 | prashantss@deepfoods.com | Linux | Prashant |
| i-0e705ce12b3f3c22c | D AWSCTX01 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-082478421d27dbda6 | D AWSCTX35 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-06c7d2408e3bfed45 | D AWSCTX44 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-05f0ff0b5b37c748c | Ignition IIOT | 1D | 1M | 9099827727 | niravad@tasktower.net | Windows | Hitesh |
| i-cda79110 | Voice Freepbx Indikitch | 1D | 1M | 8306496543 | nayanbg@teamlocus.net | Linux | Nayan Gohel |
| i-0d287cde41ffd428b | AWSCTX43 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-069817a6ee7bb98b7 | Cisco CRV Router | 1D | 1M | 8866112655 | bhargavmh@teamlocus.net | Linux | Bhargav Hingu |
| i-01d642749ac07ff5d | D AWSCTX46 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0e947f9126da59424 | D AWSCTX47 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0a6b4370a75d4119f | Grocerybabu Website Laravel | 1D | 1M | 8109650953 | vijaybd@tasktower.net | Linux | Vijay Dwivedi |
| i-04dac84c9c2aad126 | D AWSCTX53 | 1D | 1M | 7405765456 | brijeshnp@tasktower.net | Windows | Brijesh Patel |
| i-02e778915e858477e | AWSDC03 | 1D | 1M | 7405765456 | ankitrr@tasktower.com | Windows | Ankit Raval |
| i-03fec8d3350850934 | TT Allwebsites Virtual | 1D | 1M | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-05d0c123f9af4c506 | D AWSCTX45 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-03cb94e0cd429b8ac | Grocerybabu Website | 1D | 1M | 8109650953 | vijaybd@tasktower.com | Linux | Vijay Dwivedi |
| i-0ecd7c0b969964198 | D AWSCTX37 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0dd22bf94bd892b12 | Python Testing | 1D | 1M | 9574000644 | Bhargavvp@tasktower.com | Linux | Bhargav |
| i-078a21081a5f0ba14 | D AWSCTX34 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-da412a07 | TT AWSITTower Zone Brij (BJ) | 1D | 1M | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-0eeb83a385e7936f4 | D AWSCTX55 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0db2b691d5c793b43 | D Terminal Server Client Side | 1D | 1M | 7405765456 | brijeshnp@tasktower.net | Windows | Brijesh Patel |
| i-03f529cfad4225e22 | D AWSCTX54 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-0af9c2d512fa47d32 | Zimbra Mail Gobravo | 1D | 1M | 9974959142 | mayurvm@teamlocus.net | Linux | Mayur Merai |
| i-0f5ee836a2a29d74a | D AWSCTX40 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-00c45feff4e01e9be | TT Allwebsites DB Mayur | 1D | 1M | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-0bf798f0b8035e2de | UniFi Controller | 1D | 1M | 8866112655 | bhargavmh@teamlocus.net | Linux | Bhargav Hingu |
| i-0581ec9d71ea98b6b | D AWSCTX48 | 1D | 1M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-4affbd97 | Pandoarch Database Server | 1D | 3M | 9427042464 | nishant2852@gmail.com | Windows | Nishant Shah |
| i-094aee01ba961a0fa | TL AWSTLSRVC - Mayur | 1D | 3M | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |
| i-0326c24affb3bce9b | ICPL TALLY | 1D | 3M | - | - | Windows | ICPL |
| i-0b3a83d5914222a9a | D AWSWINDB03 | 1D | 3M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-00f83160321e5fcf3 | D AWSAPTDB02 | 1D | 3M | 9925035568 | brijeshnp@tasktower.com | Windows | Brijesh Patel |
| i-04d0ce9d7a412213a | TT AWSTTSQL | 1D | 3M | 9974959142 | mayurvm@teamlocus.net | Windows | Mayur Merai |

## 6.2 Steps to execute the DR Plan B: (Please refer to the Figures for more details)

You must use the AWS Backup service in order to execute the DR Plan B and it will launch a new EC2 instance by following the EC2 instance launch wizard. Use this Plan if you want to recover overall server.

**Step 1:** Identify the instance ID of the affected instance and note down the details such as VPC, Subnet, Security Group, Public IP, Private IP, Tags, Key-Pair, IAM Role, etc.

**Step 2:** Go the AWS Backup service and click on the protected resources tab from the left panel which opens the list of all the resources that are protected by the AWS backup service. (Refer: Figure 6: DR Plan B Step (2-3).Figure 6)

**Step 3:** From the list of protected resources search the instance ID which you need to recover as noted in step 1 and click on the resource ID so that it opens the particular protected resource. (Refer: Figure 6)

**Step 4:** AWS Backup creates AMI for the protected resources and as per the rule retention we can get the restore point, you can check the creation time to know point in time restore. In this plan we are taking daily backup so we have 1 restore point in 1 Day (i.e. for 15 Days retention we have 15 restore points per resource). (Refer: Figure 7)

**Step 5:** After selecting appropriate restore point you can go ahead and click on restore button on the right side of the panel window. (Refer: Figure 7)

**Step 6:** In the Restore window we need to select different options in order to create/launch new instance/resource as per the option you select. You can have option to select the instance type or keep the same instance type that of older instance. (Refer: Figure 8)

**Step 7:** You must select the VPC from the dropdown option or keep same as that of older instance. (Refer: Figure 8)

**Step 8:** You may optionally select subnet or keep subnet same as that of older subnet. (Refer: Figure 8)

**Step 9:** Optionally, select the security group in this step. (Refer: Figure 8)

**Step 10:** In this step you can select the role that newly created instance will assume so it’s very important to select proper role for the instance if application working in this instance is using some role for their operations. If you want to keep the older role with this newly restored instance then you can choose the option “Restore with original IAM role”. (Refer: Figure 8)

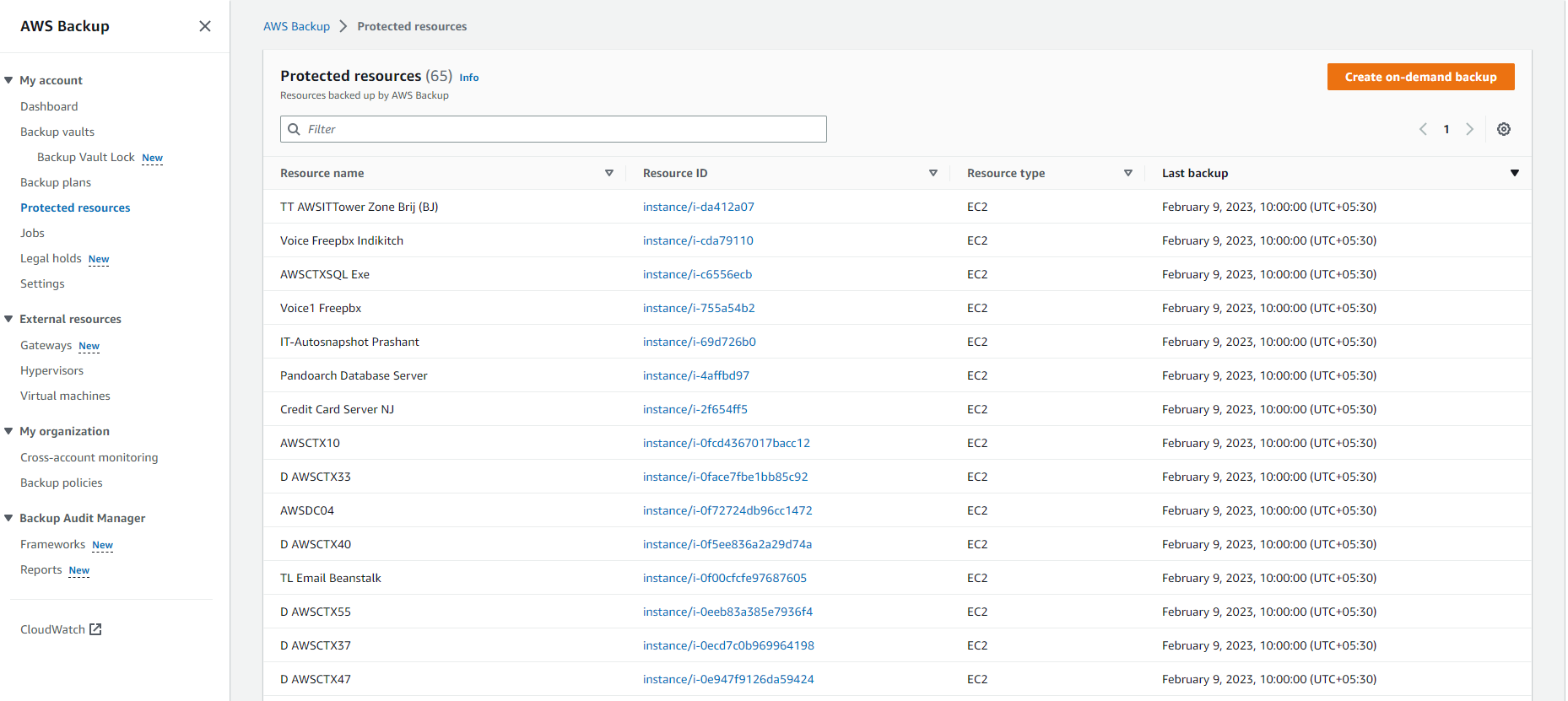
**Step 11:** Restore role is very different than the role in the step 10 because restore role is assumed by the AWS backup service to launch instance or the actions that need to be performed by the AWS Backup service to restore the resource. You can go ahead with default role which automatically creates one role which have appropriate permissions to carry out the restoration task or if you have created any role then you can use this role from the choose IAM role button. (Refer: Figure 8)

**Step 12:** This is purely optional step if you want to give any additional settings for the launched server like termination protection, Shutdown behavior, user data, tenancy, placement group, etc. (Refer: Figure 9)

**Step 13:** After entering all the details you can click on the restore button at the bottom of the panel to restore the resource. (Refer: Figure 9)

**Step 14:** After clicking on the restore button you will get the new instance launched in the EC2 console, you can go ahead and check the details and modify those details in the locations like prefix list, security groups so that the resources those are accessing this server will still able to access the resource with new public or private IP.

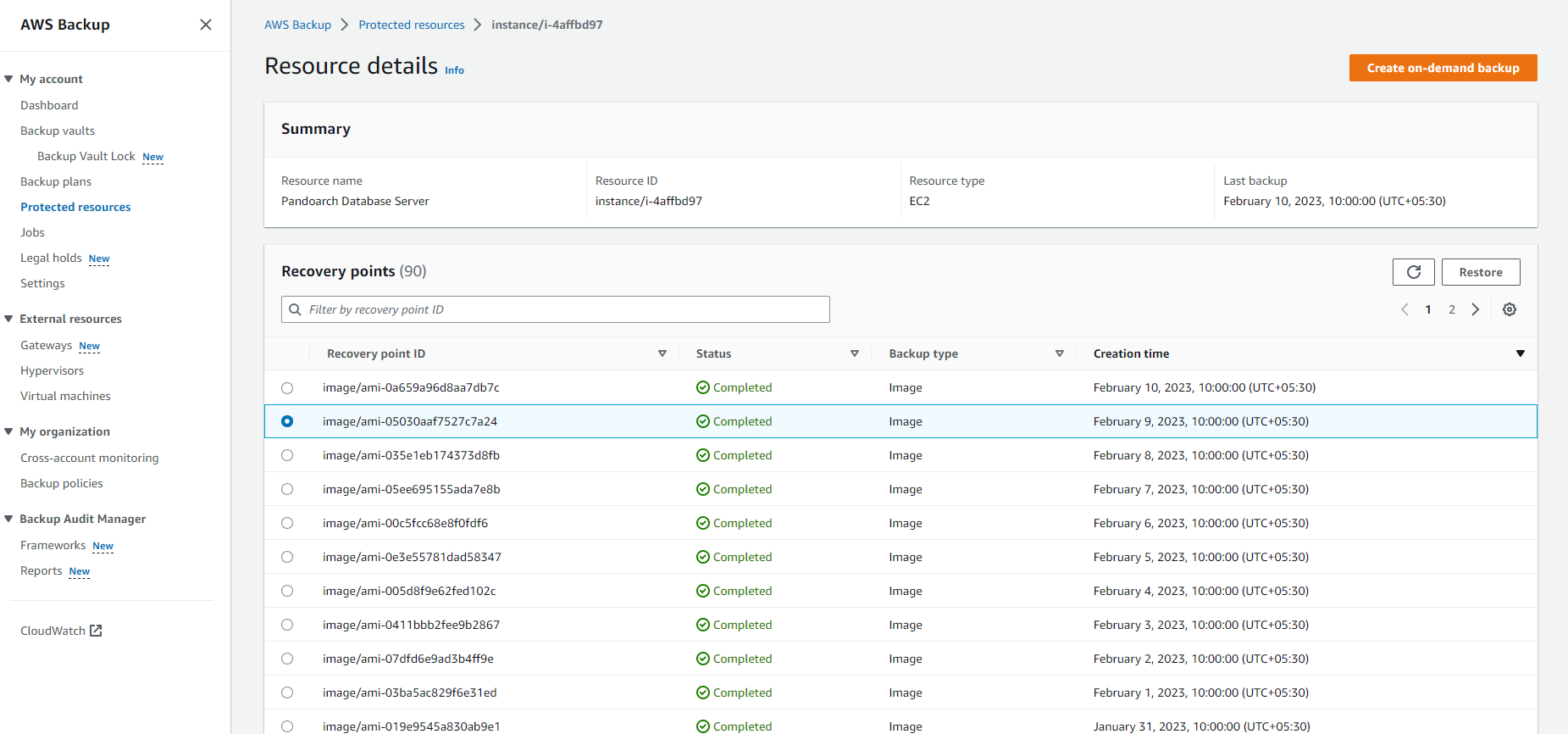
**Step 15:** This restore may not provide the instance with all the tags that are used by the organizational tag policy so you need to manually tag the all the resources after the resource gets created.



**2**

**3**

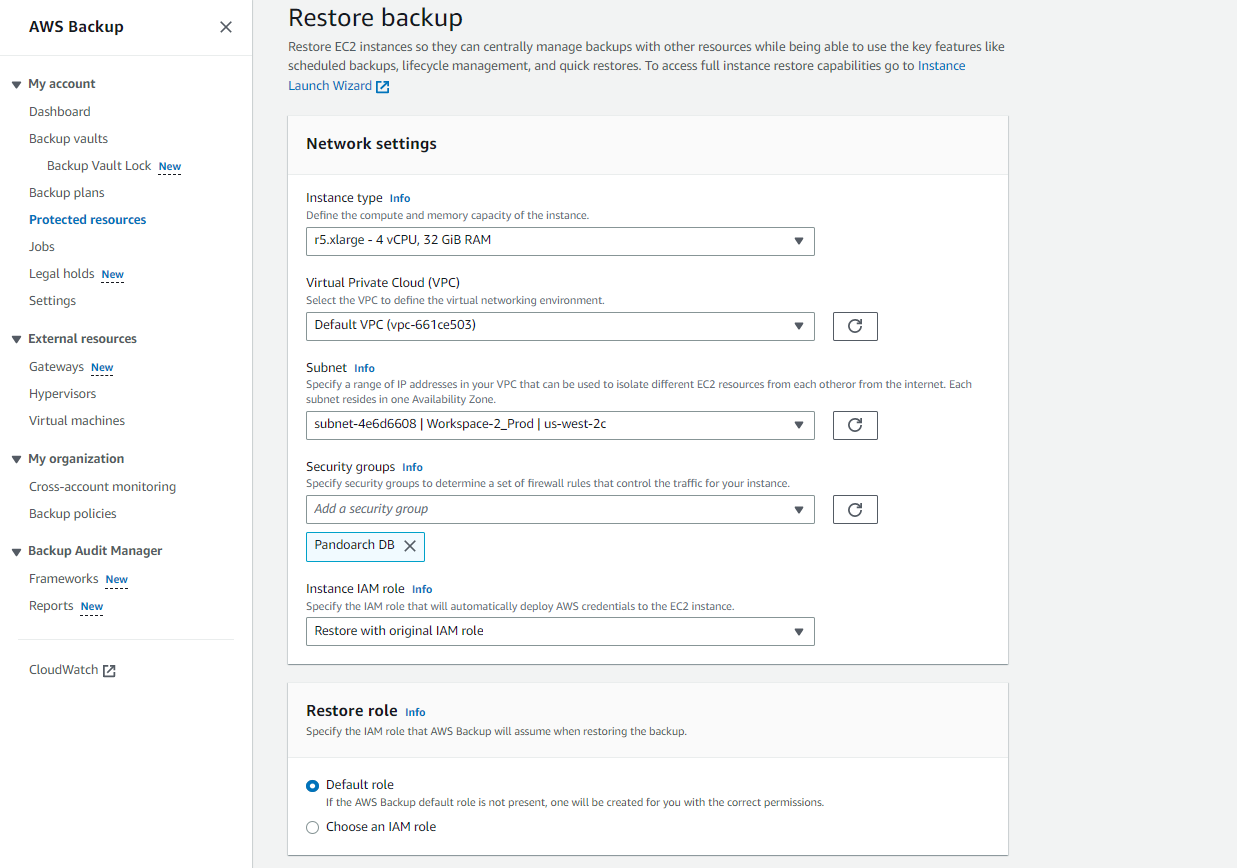
Figure 6: DR Plan B Step (2-3).



**4**

**5**

Figure 7: DR Plan B Step (4-5).



**11**

**10**

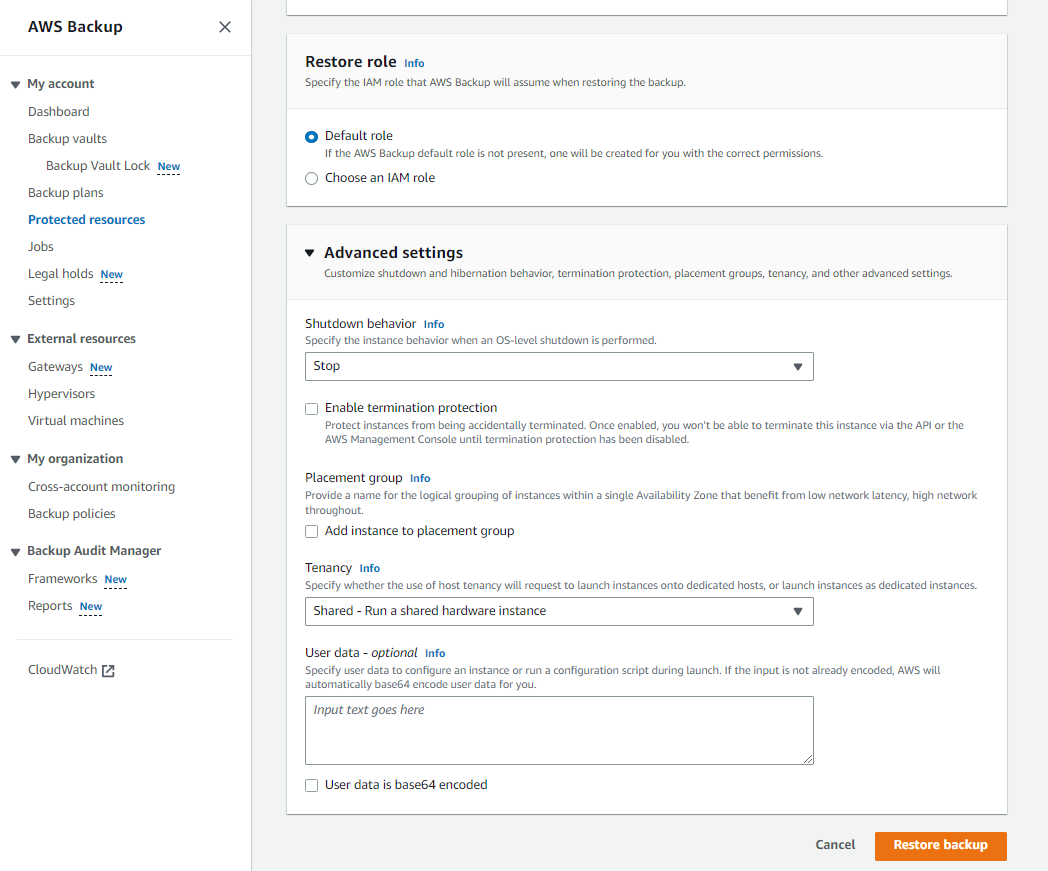
**9**

**8**

**7**

**6**

Figure 8: DR Plan B Step (6-11).



**13**

**12**

Figure 9: DR Plan B Step (12-13).

# DR Plan C

## 7.1 Consideration before executing this plan:

1. You can go for this Plan in case you don’t have any option to have DR Plan A and B that means you are not having access to AWS backup restore points and also the snapshots in EC2 console. This is in case of overall AWS infrastructure failure due to number of factors either from AWS side or our side.
2. This plan involves on-premise infrastructure to use actively in the DR process.
3. As we are taking backup at on-premise SMB servers so, we are recovering from those backups in case of disaster strikes the AWS infrastructure.
4. You need to consider that we do not have backup of all the servers to on-premise so we have limited options to recover from this DR Plan but as this is the worst case scenario plan which we may be implementing.
5. We need to consider the fact that we have the backup for databases that we can recover to a DB server but for application you need to create and deploy the application server with the help of developer.
6. We will be having two different methods to execute this plan:
   1. Restoring all the databases from on-premise to AWS/Other cloud providers.
   2. Restoring all the databases to a VM that you can create on-premises.

## 7.2 Backup strategy used for on-premise backup

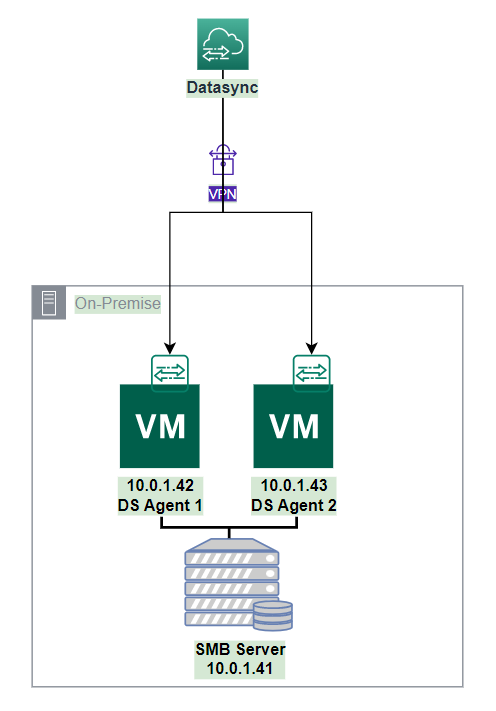


Figure 10: Datasync on-premise backup.

* AWS Datasync service is used to sync data from the S3 buckets from AWS to on-premise SMB drive as shown in Figure 10 where we have 2 VM’s where datasync agent is installed to perform the datasync task execution.
* This data synchronization happens through VPN so that we can access the SMB by using private IP of the VM.
* All the details about the datasync task executions and schedules are as described in Table 3.
* You can find the folder hierarchy and the data which you want to restore from on-premise in Figure 11.

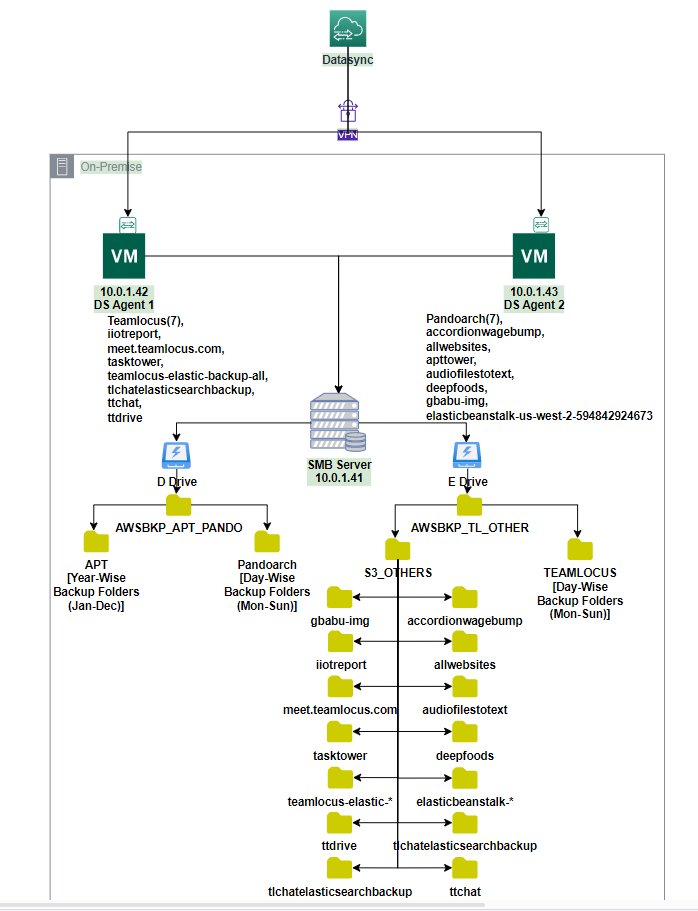


Figure 11: On-premise folder hierarchy.

Table 3: Datasync Task Details

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Time (UTC)** | **Task Name** | **Task ID** | **Source** | **Destination** |
| 12:30 AM | S3-Datasync-Backup-iiotreport | task-0588bbba5fc7b1dc2 | s3://iiotreport/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/iiotreport/ |
| 12:45 AM | S3-Datasync-Backup-meet.teamlocus.com | task-05aab4948520d397c | s3://meet.teamlocus.com/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/meet.teamlocus.com/ |
| 1:00 AM | S3-Datasync-Backup-tlchatelasticsearchbackup | task-00b5c189248814809 | s3://tlchatelasticsearchbackup/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/tlchatelasticsearchbackup/ |
| 1:15 AM | ttchat | task-0ae58f05e64393478 | s3://ttchat/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/ttchat/ |
| 1:45 AM | S3-Datasync-Backup-tasktower | task-0916506ef5be10ee4 | s3://tasktower/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/tasktower/ |
| 2:15 AM | S3-Datasync-Backup-teamlocus-elastic-backup-all | task-0bc236fbccd6a970a | s3://teamlocus-elastic-backup-all/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/teamlocus-elastic-backup-all/ |
| 10:30 AM | S3-Datasync-Backup-accordionwagebump | task-0a312b13d47453704 | s3://accordionwagebump/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/accordionwagebump/ |
| 10:45 AM | S3-Datasync-Backup-allwebsites | task-050b667330d99ab9e | s3://allwebsites/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/allwebsites/ |
| 11:00 AM | S3-Datasync-Backup-apttower | task-08fc1b3ce030053fd | s3://apttower/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/apttower/ |
| 11:15 AM | S3-Datasync-Backup-audiofilestotext | task-0a50a78e8d2dfbdb3 | s3://audiofilestotext/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/audiofilestotext/ |
| 11:30 AM | S3-Datasync-Backup-elasticbeanstalk-us-west-2-594842924673 | task-08766d631b7a2fbaf | s3://elasticbeanstalk-us-west-2-594842924673/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/elasticbeanstalk-us-west-2-594842924673/ |
| 11:45 AM | S3-Datasync-Backup-gbabu-img | task-0b6d78c0eafb009a7 | s3://gbabu-img/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/gbabu-img/ |
| 11:52 AM | Teamlocus-Datasync-Backup-Application | task-0ae1884a7714c6cc1 | s3://teamlocusdbbackup/Backup/Application/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Application/ |
| 12:00 PM | S3-Datasync-Backup-deepfoods | task-0070a073eaede78a6 | s3://deepfoods/ | smb://10.0.1.41/AWSBKP\_TL\_OTHER/S3\_OTHERS/deepfoods/ |
| 06:30 AM, Tue | Pando-Datasync-Backup-Tuesday | task-04b5d2b837a04b6e1 | s3://pandoarchdbbkp/Backup/Tuesday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Tuesday/ |
| 06:30 AM, Fri | Pando-Datasync-Backup-Friday | task-0fdeafcda0aea2222 | s3://pandoarchdbbkp/Backup/Friday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Friday/ |
| 06:30 AM, Mon | Pando-Datasync-Backup-Monday | task-04fd4d112d5d711c2 | s3://pandoarchdbbkp/Backup/Monday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Monday/ |
| 06:30 AM, Sun | Pando-Datasync-Backup-Sunday | task-0d0bf496718fa53ed | s3://pandoarchdbbkp/Backup/Sunday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Sunday/ |
| 06:30 AM, Thu | Pando-Datasync-Backup-Thursday | task-0e102f1d6729b73e3 | s3://pandoarchdbbkp/Backup/Thursday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Thursday/ |
| 06:30 AM, Wed | Pando-Datasync-Backup-Wednesday | task-09382a88bd6274fd1 | s3://pandoarchdbbkp/Backup/Wednesday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Wednesday/ |
| 06:30 AM, Sat | Pando-Datasync-Backup-Saturday | task-0d18bc7bb48840445 | s3://pandoarchdbbkp/Backup/Satuarday/ | smb://10.0.1.41/awsbkp\_apt\_pando/PANDOARCH/Satuarday/ |
| 01:30 PM, Fri | Teamlocus-Datasync-Backup-Friday | task-035be3096597f9fca | s3://teamlocusdbbackup/Backup/Friday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Friday/ |
| 01:30 PM, Mon | Teamlocus-Datasync-Backup-Monday | task-02b9f194f2286df03 | s3://teamlocusdbbackup/Backup/Monday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Monday/ |
| 01:30 PM, Sat | Teamlocus-Datasync-Backup-Saturday | task-0b973d79925aa03db | s3://teamlocusdbbackup/Backup/Satuarday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Satuarday/ |
| 01:30 PM, Sun | Teamlocus-Datasync-Backup-Sunday | task-01eefa8671a50afec | s3://teamlocusdbbackup/Backup/Sunday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Sunday/ |
| 01:30 PM, Thu | Teamlocus-Datasync-Backup-Thursday | task-059d589c9be0de508 | s3://teamlocusdbbackup/Backup/Thursday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Thursday/ |
| 01:30 PM, Tue | Teamlocus-Datasync-Backup-Tuesday | task-0042453f32ae0d48b | s3://teamlocusdbbackup/Backup/Tuesday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Tuesday/ |
| 01:30 PM, Wed | Teamlocus-Datasync-Backup-Wednesday | task-077ada0eeb37eb95f | s3://teamlocusdbbackup/Backup/Wednesday/ | smb://10.0.1.41/awsbkp\_tl\_other/TEAMLOCUS/Wednesday/ |

## 7.3 Steps to execute the DR Plan C: (Please refer to the Figures for more details)

**Step 1:** Firstly, you need to decide whether you want to use the AWS/cloud or local to run your workloads and take proper steps.

**Step 2:** If you want to restore to AWS cloud then you can restore by creating task in datasync which will copy data from on-premise to S3.

**Step 3:** If you need to restore to local VM then you can copy create application and database server at local on-premise and copy data from the SMB to local VM which you created and run the workloads from the on-premise infrastructure.

# Project Teamlocus DR Plans

## 8.1 Architectural overview of project Teamlocus Disaster Recovery

* The overall backup plan architecture for all the different DR Plans is shown in Figure 12.
* In Figure 12 there are 3 different sections for three different types of Backup plans namely Backup Plan: A, Backup Plan: B, Backup Plan: C.
* You can execute any DR plan as per the scenario by referring to the Table 1 and first select the type of DR plan you need to execute.
* You can refer to the steps mentioned in 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for DR Plan A and also refer Table 4 for getting information about the prerequisite to execute Plan A.
* If the volume you want to restore is not available in Table 4 then it’s not possible to execute the DR Plan A. So please use the DR Plans sections to decide the DR plan should be used.
* We do have some critical DB backup for DR Plan A but if you want to restore any other data you can make use of S3 bucket backup files to restore apart from this DR Plan A.
* If you don’t have option for DR Plan A then you can go for DR Plan B and follow the steps mentioned in 6.2 Steps to execute the DR Plan B: (Please refer to the Figures for more details)
* In case of worst case scenario of not having any AWS resources to recover the workload, then you have final DR Plan C, which you can execute as per the steps mentioned in 7.3 Steps to execute the DR Plan C: (Please refer to the Figures for more details).

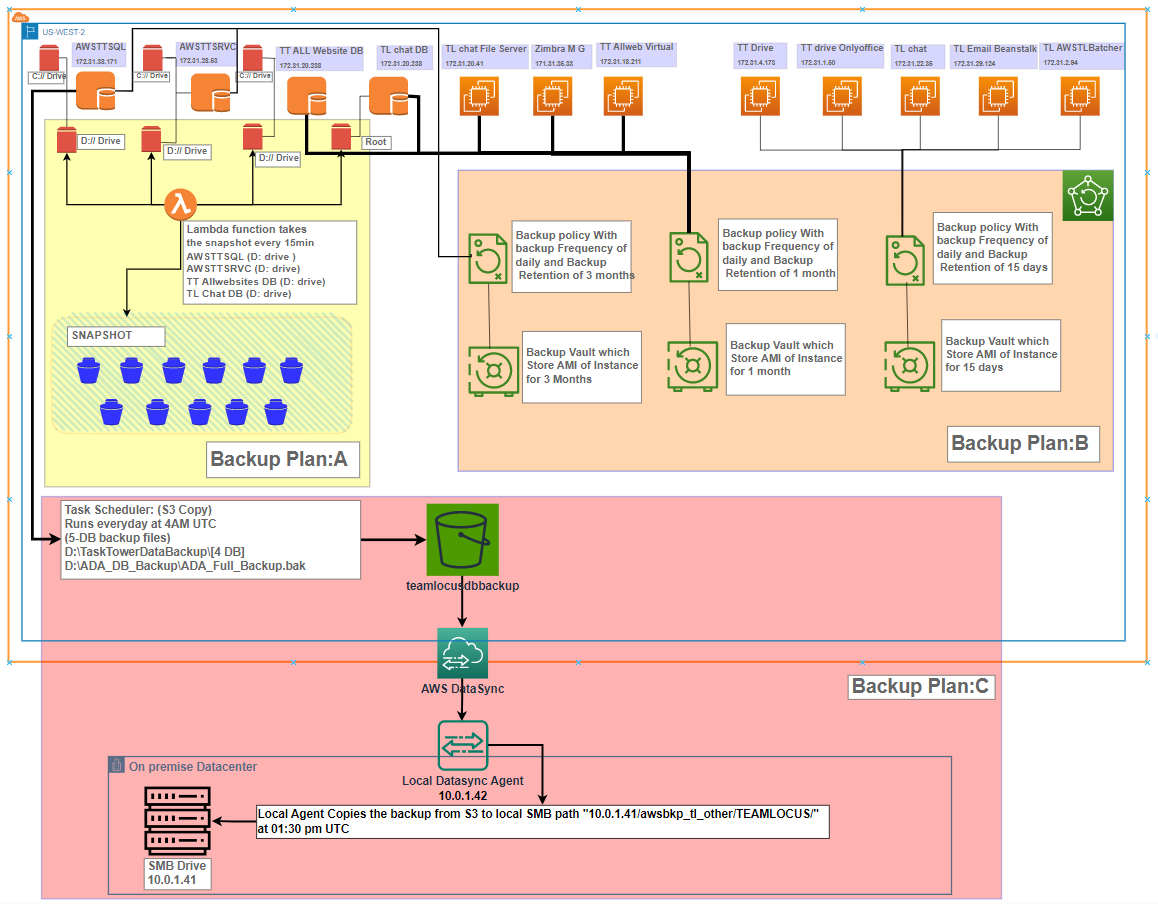


Figure 12: Project Teamlocus Backup Plan Architecture.

## 8.2 Steps to execute the DR Plan A:

Identify the teamlocus DB server that we will have to execute DR plan A if teamlocus server fails due to any failure as mentioned in Table 1.

* We have 4 DB server AWSTTSQL, AWSTTSRVC, TT All-Website DB and TL chat DB . All DB server have two EBS volume each except that of TL chat DB.
* With the help Lambda function we are taking a snapshot of each protected volume at every 15 minutes as mentioned in Table 4.
* In case of any issue arises due to failure we can restore the volume from latest snapshot in order to meet the RPO of 15 minutes.
* Please refer 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for more details about the detail procedures about the Plan A execution along with the Table 4.

## 8.3 Steps to execute the DR Plan B:

Identify the teamlocus servers that failed due to any issue as mentioned in the Table 1, we can execute DR plan B.

* We have 8 application servers for teamlocus project.
* If any of the server fails due to any issue as mentioned in Table 1 you can restore by DR Plan B using AWS Backup service.
* AWS backup service creates AMI for the AWSTTSRVC and AWSTTSQL every day and keeps the retention for 3 months.
* TT Allwebsites DB, TL Chat DB,TL chat file server, Zimbra Mail Gobravo, TT AllWebsites virtual servers has frequency of daily and backup retention of 1 month.
* TT drive, TT drive onlyoffice, TL chat, TL Email Beanstalk, TL AWSTL Batcher has frequency of daily and backup retention of 15 days.
* For more information about the Backup Frequency and Backup Retention you can refer to the Table 2.
* We can launch instance from that AMI immediately.
* AWS Backup service uses tags to filter out the instances which needs to backup.
* So, it’s very important to add the tags after the new instance launched after the execution of DR Plan B.

Table 4: Teamlocus Servers Volume backup information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name of Servers** | **Instance ID** | **Volumes** | | | | | |
|  |  | **Nos.** | **Size of Volume** | **Volume ID** | **Backup Taken** | **Backup Frequency** | **Backup Retention** |
| AWSTTSRVC | i-094aee01ba961a0fa | 2 | C: 100 | vol-01669311aedcbf3f6 | NO | - | - |
| D: 2500 | vol-041892764274ae5e7 | Yes | 15 Min | 7 Days |
| AWSTTSQL | i-04d0ce9d7a412213a | 2 | C: 100 | vol-036277956faf0812b | NO | - | - |
| D: 700 | vol-0ec9570e7e704825e | Yes | 15Min | 7 Days |
| TT Allwebsites DB | i-00c45feff4e01e9be | 2 | C: 300 | vol-0b809e81397f5c7d0 | NO | - | - |
| D: 500 | vol-0bdca73f17fc05560 | Yes | 15Min | 7 Days |
| TL Chat DB | i-04d0ce9d7a412213a | 1 | C: 100 | vol-034bcd050a1c05f6a | Yes | 15Min | 7 Days |

## 8.4 Steps to execute the DR Plan C:

In this case if overall AWS infrastructure goes down we can execute this plan. In this case we would have backup of database on on-premise we can recover either on on-premise or AWS/other clouds.

* We have all backup of Teamlocus DB locally in NJ on SMB server 10.0.1.41
* We can take the backup or revert back those backup on on-premise from SMB server or either on AWS cloud using AWS datasync service.
* You can refer to Figure 11 for more detailed backup location information about the local VM and SMB and then you can recover from the SMB to desired location of your choice.

# Project Pandoarch DR Plans

## 9.1 Architectural overview of project Pandoarch Disaster Recovery

* The overall backup plan architecture for all the different DR Plans is shown in Figure 13.
* In Figure 13 there are 3 different sections for three different types of Backup plans namely Backup Plan: A, Backup Plan: B, Backup Plan: C.
* You can execute any DR plan as per the scenario by referring to the Table 1 and first select the type of DR plan you need to execute.
* You can refer to the steps mentioned in 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for DR Plan A and also refer for getting information about the prerequisite to execute Plan A.
* If the volume you want to restore is not available in Table 5 then it’s not possible to execute the DR Plan A. So please use the DR Plans sections to decide the DR plan should be used.
* We do have some critical DB backup for DR Plan A but if you want to restore any other data you can make use of S3 bucket backup files to restore apart from this DR Plan A.
* If you don’t have option for DR Plan A then you can go for DR Plan B and follow the steps mentioned in 6.2 Steps to execute the DR Plan B: (Please refer to the Figures for more details)
* In case of worst case scenario of not having any AWS resources to recover the workload then you has final DR Plan C, which you can execute as per the steps mentioned in 7.3 Steps to execute the DR Plan C: (Please refer to the Figures for more details).

**9.2 Steps to execute the DR Plan A:**

Identify the Pandoarch DB server that we will have to execute DR plan A if Pandoarch server fails due to any failure as mentioned in Table 1.

* We have 1 DB server Pandoarch DB. This DB server has two EBS volumes namely vol-506b31d0 ( D-drive) and vol-1082f090 (E-drive).
* With the help Lambda function we are taking a snapshot of this protected volume at every 15 minutes as mentioned in Table 5.
* In case of any issue arises due to failure we can restore the volume from latest snapshot in order to meet the RPO of 15 minutes.
* Please refer 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for more details about the detail procedures about the Plan A execution along with the Table 5

**9.3 Steps to execute the DR Plan B:**

Identify the pandoarch servers that failed due to any issue as mentioned in the Table 1, we can execute DR plan B.

* We have 3 servers for pandoarch project.
* If any of the server fails due to any issue as mentioned in Table 1 you can restore by DR Plan B using AWS Backup service.
* AWS backup service creates AMI for the mentioned servers every day and keeps the retention for as described in Table 2
* For more information about the Backup Frequency and Backup Retention you can refer to the Table 2.
* We can launch instance from that AMI immediately.
* AWS Backup service uses tags to filter out the instances which needs to backup.
* So, it’s very important to add the tags after the new instance launched after the execution of DR Plan B.

**9.4 Steps to execute the DR Plan C:**

In this case if overall AWS infrastructure goes down we can execute this plan. In this case we would have backup of database on on-premise we can recover either on on-premise or AWS/other clouds.

* We have all backup of Pandoarch DB locally in NJ on SMB server 10.0.1.41
* We can take the backup or revert back those backup on on-premise from SMB server or either on AWS cloud using AWS datasync service.
* You can refer to Figure 11 for more detailed backup location information about the local VM and SMB and then you can recover from the SMB to desired location of your choice.

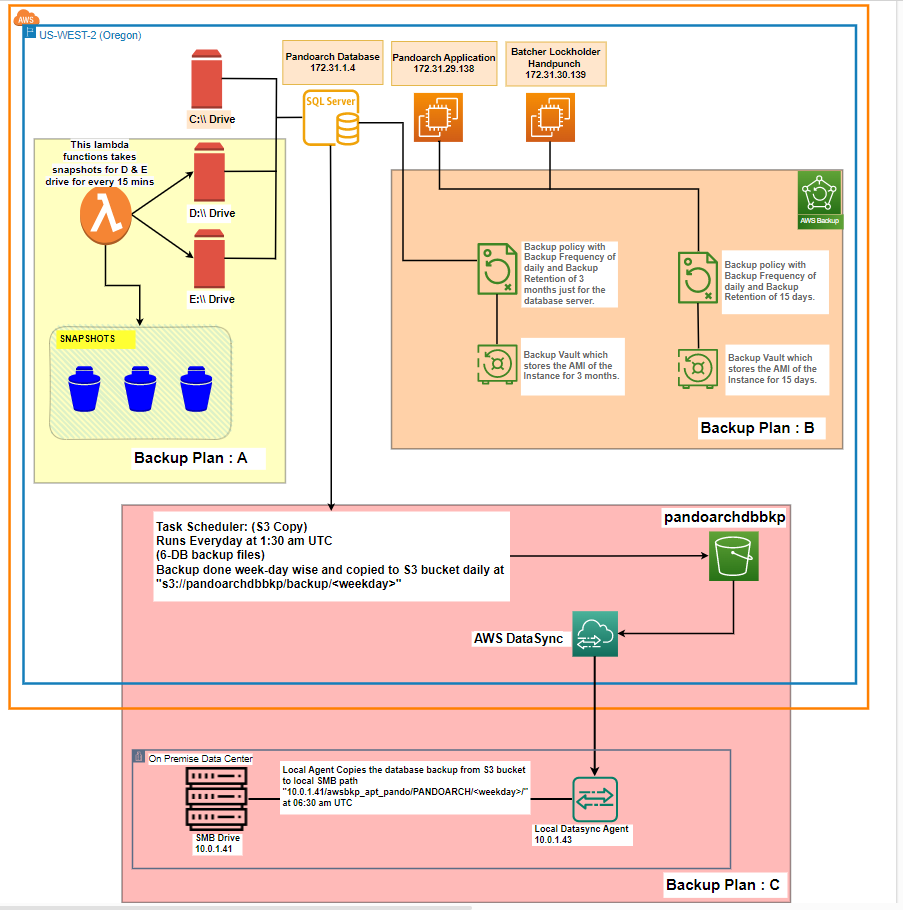


Figure 13: Project Pandoarch Backup Plan Architecture.

Table 5: Pandoarch Servers Volume backup information

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name of Servers** | **Instance ID** | **Volumes** | | | | | |
|  |  | **Nos.** | **Size of Volume** | **Volume ID** | **Backup Taken** | **Backup Frequency** | **Backup Retention** |
| Pandoarch Database | i-4affbd97 | 3 | C: 150 | vol-c5683245 | NO | - | - |
| D:500 | Vol-506b31d0 | Yes | 15 min | 7 Days |
| E: 1000 | vol-1082f090 | Yes | 15 Min | 7 Days |

1. **Project APT DR Plans**

**10.1 Architectural overview of project APT Disaster Recovery**

* The overall backup plan architecture for all the different DR Plans is shown in Figure 14.
* In Figure 14 there are 3 different sections for three different types of Backup plans namely Backup Plan: A, Backup Plan: B, Backup Plan: C.
* You can execute any DR plan as per the scenario by referring to the Table 1 and first select the type of DR plan you need to execute.
* You can refer to the steps mentioned in 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for DR Plan A and also refer Table 6 for getting information about the prerequisite to execute Plan A.
* If the volume you want to restore is not available in Table 6 then it’s not possible to execute the DR Plan A. So please use the DR Plans sections to decide the DR plan should be used.
* We do have some critical DB backup for DR Plan A but if you want to restore any other data you can make use of S3 bucket backup files to restore apart from this DR Plan A.
* If you don’t have option for DR Plan A then you can go for DR Plan B and follow the steps mentioned in 6.2 Steps to execute the DR Plan B: (Please refer to the Figures for more details)
* In case of worst case scenario of not having any AWS resources to recover the workload then you has final DR Plan C, which you can execute as per the steps mentioned in 7.3 Steps to execute the DR Plan C: (Please refer to the Figures for more details).

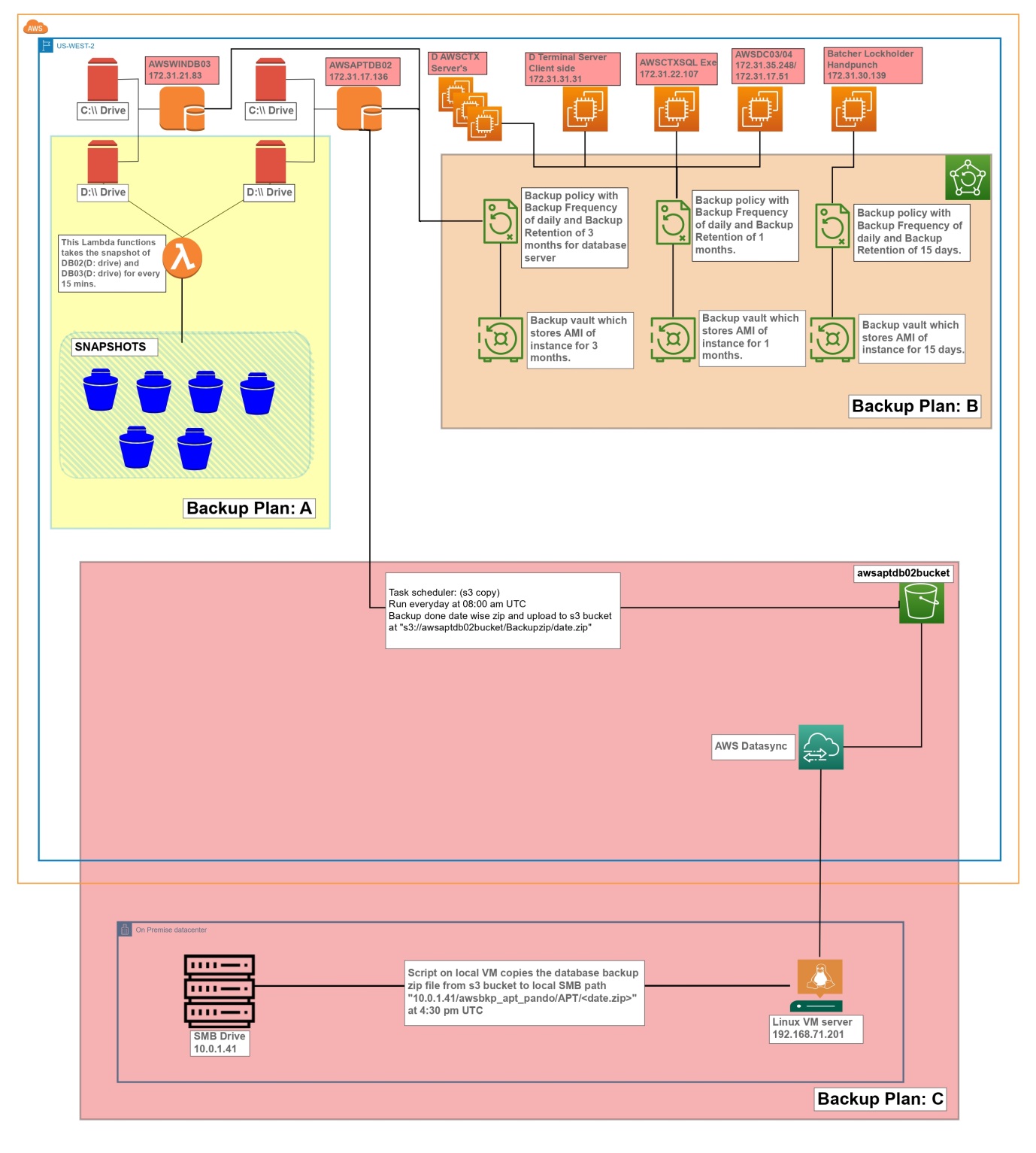


Figure 14: Project APT Backup Plan Architecture.

## 10.2 Steps to execute the DR Plan A:

Identify the APT database servers that we will have to execute DR plan A if APT servers fails due to any failure as mentioned in Table 1.

* We have 2 DB servers AWSWINDB03 AND AWSAPTDB02.
* With the help Lambda function we are taking snapshots of each protected volume at every 15 minutes as mentioned in Table 6
* In case of any issue arises due to failure we can restore the volume from latest snapshot in order to meet the RPO of 15 minutes.
* Please refer 5.2 Steps to execute the DR Plan A: (Please refer Figures for more details) for more details about the detail procedures about the Plan A execution along with the Table 6

**10.3 Steps to execute the DR Plan B:**

Identify the APT servers that failed due to any issue as mentioned in the Table 1, we can execute DR plan B.

* We have 30 servers for APT project.
* If any of the server fails due to any issue as mentioned in Table 1 you can restore by DR Plan B using AWS Backup service.
* AWS backup service creates AMI for all the servers every day and keeps the retention as mentioned in Table 2.
* For more information about the Backup Frequency and Backup Retention you can refer to the Table 2.
* We can launch instance from that AMI immediately.
* AWS Backup service uses tags to filter out the instances which needs to backup.
* So, it’s very important to add the tags after the new instance launched after the execution of DR Plan B.

**10.4 Steps to execute the DR Plan C:**

In this case if overall AWS infrastructure goes down we can execute this plan. In this case we would have backup of database on on-premise we can recover either on on-premise or AWS/other clouds.

* We have all backup of Pandoarch DB locally in NJ on SMB server 10.0.1.41
* We can take the backup or revert back those backup on on-premise from SMB server or either on AWS cloud using AWS datasync service.
* You can refer to Figure 11 for more detailed backup location information about the local VM and SMB and then you can recover from the SMB to desired location of your choice.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **Name of Servers** | **Instance ID** | **Volumes** | | | | | |
|  |  | **Nos.** | **Size of Volume** | **Volume ID** | **Backup Taken** | **Backup Frequency** | **Backup Retention** |
| AWSWINDB03 | i-0b3a83d5914222a9a | 2 | C: 100 | vol-0938dce817c588a32 | NO | - | - |
| D: 4096 | vol-05ca07f9a99e679c9 | Yes | 15 Min | 7 Days |
| AWSAPTDB02 | i-00f83160321e5fcf3 | 2 | C: 100 | vol-000c453405c8e9d2c | NO | - | - |
| D: 3000 | vol-0b4cc01686c278042 | Yes | 15Min | 7 Days |

Table 6: APT Servers Volume backup information

# Thanks