Cognito Disaster Recovery Process

Overview

This document is intended to provide the process to recover the Vectra® service in the event of the failure of the Primary Brain in DC1.

Assumptions:

- Backup (warm spare) brain of equal or comparable scoping is available in another location, accessible to all Vectra appliances deployed.
- DNS TTL for the Vectra domain is set to 120 seconds.
- Backups have been configured on the primary Brain for both Brain-to-Brain, as well as external SCP server.

Summary of steps to validate this process are below. In an actual failure scenario, only steps 4-6 are required for recovery and steps 8-13 to revert back to Primary Brain in DC1.

PROCESS OVERVIEW

Step	Step Description
1	Log into DC1 Brain and confirm it is operational with successful connectivity to all Sensors configured
2	Confirm DC1 Brain automatic backups are configured and at least one recent backup has been stored on DC2 Brain
3	Disconnect or disable network port connected to MGT1 on the DC1 Brain appliance to simulate a failure event
4	Log into DC2 Brain and initiate restore procedure to restore the Brain backup
5	Reconfigure DNS for Vectra.domain.com to point to backup Brain IP address
6	Log into DC2 Brain and confirm it is operational with successful connectivity to all Sensors configured (~10 minutes)
7	Reconnect MGT1 on the DC1 Brain to simulate recovery in DC1
8	Log into DC2 Brain and confirm it is still operational with successful connectivity to all Sensors configured
9	Perform manual CLI-based backup of DC2 Brain and restore to DC1 Brain
10	Reconfigure DNS for Vectra.domain.com to point to primary Brain IP address
11	Perform CLI reboot on backup Brain
12	Log into DC1 Brain and confirm it is operational with successful connectivity to all Sensors configured (~10 minutes)
13	Confirm DC1 Brain backups are still configured
14	Reconfigure Brain-to-Brain backup with new backup Brain token
15	Disable automatic backups on the backup Brain and re-configure to accept Brain-to-Brain backups from DC1

Detailed Steps

Step 1

Log into DC1 Brain and confirm it is operational with successful connectivity to all Sensors configured.

- Navigate a browser to https://vectra.domain.com
- Log in and click on “Traffic” in the main navigation pane
- Verify active traffic with recent Last Connection timestamps

Step 2

Confirm DC1 Brain automatic backups are configured and at least one recent backup has been stored on DC2 Brain.

- Use SSH to access the DC1 Brain:

```
ssh vectra@vectra.domain.com
```

- Use the **backup show** command to view current backup configuration:

```
backup show
```

- If a Last Copy Failure timestamp is present and is from the most recent backup, resolve any issues preventing successful copy to SCP and/or DC2 Brain, and use the **backup run** command to create a new backup. Ensure there are no new copy failures returned via error message(s).

Step 3

Disconnect or disable network port connected to MGT1 on the DC1 Brain appliance to simulate a failure event.

- Navigate a browser to https://vectra.domain.com
- Ensure unsuccessful response from the Vectra Cognito UI

Step 4

Log into DC2 Brain and initiate restore procedure to restore the Brain backup.

- Use SSH to access the DC2 Brain:

```
ssh vectra@BackupBrainIP
```

- Use the **restore list** command to obtain the backup number of the desired backup.
- Use the **restore run** command to run the actual restore. To restore from the first backup in the list, for example:

```
restore run --local 1
```

Step 5

Reconfigure DNS for vectra.domain.com to point to backup Brain IP address.

- Point the DNS record to the IP address of the backup Brain.
- DNS TTL for vectra.domain.com is set for 120 seconds, so wait up to two minutes before moving on to Step 6.

Step 6

Log into DC2 Brain and confirm it is operational with successful connectivity to all Sensors configured.

- Navigate a browser to https://vectra.domain.com
- Click Settings in primary navigation pane and ensure the Hostname in Brain section is the IP of the backup Brain.
- Click on Traffic and ensure all sensors have Last Seen connection timestamps more recent than when the DNS change went into effect from Step 5. This may take up to 10 minutes to fully show all active tunnel connections as being up.

Step 7

Reconnect MGT1 on the DC1 Brain to simulate recovery in DC1 Brain.

- Re-establish physical or configuration-based connectivity to the DC1 Brain.

Step 8

Log into DC2 Brain and confirm it is still operational with successful connectivity to all Sensors configured.

- Navigate a browser to https://vectra.domain.com
- Click Traffic in the main navigation pane to confirm sensors are still paired and operational.

Step 9

Perform manual CLI-based backup of DC2 Brain and restore to DC1 Brain.

- Use SSH to access the DC2 Brain:

```
ssh vectra@vectra.domain.com
```

- Perform a manual backup which will be sent to the SCP backups server:

```
backup run
```

- Once completed successfully, SSH to DC1 Brain:

```
ssh vectra@PrimaryBrainIP
```

- Restore the latest backup from DC2 into DC1:

```
restore run --scp vectra@SCPServerIP:
vectra/backup_file.tar.gz.gpg
```

Note: The backup file will look something similar to **migration-5.2.2-8-0-20191209.tar.gz.gpg**. Verify file name of most recent backup on SCP server.

Step 10

Reconfigure DNS for vectra.domain.com to point to primary Brain IP address.

- Point the DNS record to the Primary Brain IP.
- DNS TTL for vectra.domain.com is set for 120 seconds, so wait up to two minutes before moving on to Step 11.

Step 11

Perform CLI reboot on backup Brain.

- Use SSH to access the DC2 Brain:

```
ssh vectra@BackupBrainIP
```

- Perform the reboot:

```
reboot
```

Note: This reboot forces the sensors to break SSH Tunnel connectivity with the backup brain so that they can re-establish connectivity with the DC1 Brain.

Step 12

Log into DC1 Brain and confirm it is operational with successful connectivity to all Sensors configured.

- Navigate a browser to https://vectra.domain.com
- Click Settings in primary navigation pane and ensure the Hostname in Brain section is the IP address of the primary Brain.
- Click on Traffic and ensure all sensors have Last Seen connection timestamps more recent than when the DNS change went into effect from Step 10. This may take up to 10 minutes to fully show all active tunnel connections as being up.

Step 13

Confirm DC1 Brain backups are still configured.

- Use SSH to access the DC1 Brain:

```
ssh vectra@vectra.domain.com
```

- Use the **backup show** command to view current backup configuration:

```
backup show
```

Step 14

Reconfigure Brain-to-Brain backup with new backup Brain token.

- Use SSH to access the DC2 Brain:

```
ssh vectra@BackupBrainIP
```

- Use the **token show** command to obtain the new backup Brain token (a new token would have generated during the restore process when switching DC2 brain as the primary brain).

```
token show
```

- Copy the token
- Use SSH to access the DC1 Brain:

```
ssh vectra@vectra.domain.com
```

- Use the **backup configure-target** command to update the DC2 token:

```
backup configure-target --brain-key token
```

- Use the **backup show** command to ensure the new token reflects in the Brain Key configuration:

```
backup show
```

Step 15

Disable automatic backups on the backup Brain and re-configure to accept Brain-to-Brain backups from DC1.

- Use SSH to access the DC2 Brain:

```
ssh vectra@BackupBrainIP
```

- Use the **backup disable** command to disable automatic backups, as we do not want both the primary and backup brain to create new backup files.

```
backup disable
```

- Use the **accept-from-brains** command to allow Brain-to-Brain backups from DC1.

```
backup accept-from-brains PrimaryBrainIP
```

VECTRA®
Security that thinks®

Email info@vectra.ai **Phone** +1 408-326-2020
vectra.ai