The Guide to...

Hosted Exchange Disaster Recovery

Green Cloud Hosting™

Hardware Configuration

CISCO FIREWALLS

The Cisco firewalls we use to manage the network are ASA models, we run them in each individual Data Centre/Cabinet applicable to the Hosted Exchange environment. Each Data Centre/Cabinet has its own primary Cisco ASA, which has live configuration trafficking to a standby unit in the same location. This ensures that the Cisco firewall is not a single failover point, as the standby unit will take over in the event of any software/hardware failure on the primary unit. The Cisco firewalls are linked over Cabinet-Cabinet/Data Centre-Data Centre direct 10Gbps links, thus internal trafficking is still available in the event of a network failure at a single/multiple locations.

BARRACUDA SPAM & VIRUS FIREWALLS

The barracuda firewalls are stored in each Data Centre/Cabinet accordingly, they are fully power/network redundant in each Data Centre/Cabinet. These are again stored across multiple locations, accepting mails at any location, this will automatically route mail through working devices should any of the devices face a software/hardware failure. The Barracuda devices are connected over 10Gbps Dark Fiber links between the different locations.

EXCHANGE HARDWARE

The Exchange servers are spread across the different locations, with each role having multiple servers in each location, for best fault tolerance practices. The Front End servers (Client Access and Hub Transport) are all virtual servers, running through a separate 10Gbps SAN on Solid State Drives, designed for optimal speed and fault tolerance. There is failover SAN and Virtual environments, designed to automatically take over in the event of failures on the primary solutions. The standby virtual environment enables us to almost instantly bring the failed servers back up and online, to work with the same configuration.

GOING FORWARD

Going forward, we are looking to further implement SSD technology in the Mailbox server configuration, this uses faster drive speeds and increases our fault tolerance against specific issues. This should enable for us to provide faster database access for the mailboxes, thus resulting in an increased performance for the clients to access their mail services. We apply the same technology across both the Exchange 2010 and 2013 environments, in order that we may provide an equally fast and fault tolerant system for clients wishing to use the latest Hosted Exchange technologies.

Software Configuration

CISCO FIREWALLS

The software configuration of the Cisco ASA firewalls, is designed in a way that limits only very particular access to the network, thus increasing network fault tolerance with only limited access. The software configuration is live-streamed to standby units with the same restrictive configuration. This ensures that on a software level, we are offering the best possible fault tolerance practices.

BARRACUDA FIREWALLS

The Barracuda firewalls have multiple levels of software fault tolerance built into the environment. The devices work as a cluster, this is an in-built process whereby 2 or more devices are in place, to live-stream the configuration between themselves, and to alert the device to be excluded from mail receipt when any issues are seen with any of the devices. We also run a cloud protection layer on the Barracuda devices, this is essentially a web based service provided through Barracuda, which ensures that even in a worst case scenario, whereby all Data Centres and devices were to be down simultaneously, we would still be able to store mail externally, ready for delivery as and when services could be resumed, thus ensuring no downtime in mail receipt to our systems is interrupted upon service resumption.

EXCHANGE CONFIGURATION

With the Exchange environment, all of the Front End servers run in a DAG Array (Database Availability Group), which means that we can spread the load across the whole environment with ease. The system automatically passes mail through based on load levels, ensuring that no servers are overloaded to cause slowness or delay mail receipt to any mailbox (es). Another benefit of the DAG environment, is that we can store live replica copies of the mailbox databases across servers in separate locations, thus meaning that we can live mount databases at other locations, should any load/downtime/outage issues be seen. This means that even if a Data Centre is down completely, we can ensure connectivity by mounting the appropriate mailbox databases on the replica systems designed for such an event, this is a nearly instantaneous step to return mail connectivity for the affected mail users. This process is instantaneous in the event of any failure, restoring service as swiftly as possible. We also run a

LOOKING AHEAD

All services are constantly updated on software levels, so that the latest updates, service packs and rollups are live as soon as possible on the live environment. We have also implement a full Vaeem backup solution behind the virtual front end infrastructure, thus meaning our virtual server backups are as often as possible with a very high and accurate level of restore capability.

Disaster Recovery Models & Processes

PROCESS IN EVENT OF DATA CENTRE OUTAGE

- The system will automatically disable remote access to the affected servers, thus routing all traffic through the working locations.
- The affected Barracuda model will be temporarily removed from the cluster, thus not told to be receiving any emails from us or externally, thus routing mail only through working locations.
- The system will automatically mount the affected databases on the working servers as local server access is not affected.
- The affected front end servers will be brought back online in a separate Data Centre virtual environment to continue with full server capacity.
- The Cisco devices at a particular site will then not have to face any traffic so that any work on these devices is not required.
- Once complete, all access is restored for the clients in the affected Data Centre.

PROCESS IN THE EVENT OF CISCO FIREWALL FAILURE

- The standby unit will immediately takeover the services, once the failure is seen on the primary unit.
- We would then proceed to physically replace the affected Cisco unit and set the standby unit as the primary unit in the process.
- We expect no downtime, and the device once fixed will be kept as a spare pending any other failures.

PROCESS IN THE EVENT OF BARRACUDA FAILURE

- If a single Barracuda device fails, the external mails and internal mails sent out will be automatically directed to only working
- We would then proceed to physically replace the affected Cisco unit and set the standby unit as the primary unit in the process.
- We expect no downtime, and the device once fixed will be kept as a spare pending any other failures.

PROCESS IN THE EVENT OF FRONT END SERVER FAILURE/MAILBOX SERVER FAILURE

- Any individual issue with a Front End or Mailbox server, is readily in place to bring backup with a minimal amount of downtime.
- With regards to the Front End servers, the replica virtual servers based in separate locations will bring the server up as soon as downtime is seen. We would then resolve the original server fault and resume to active service over time.
- With regards to the Mailbox servers, we would simply bring the databases back online in a working location. We would resolve the server fault, and then return to active service over time.

Data Centre Information & Locations

DATA CENTRE LOCATIONS

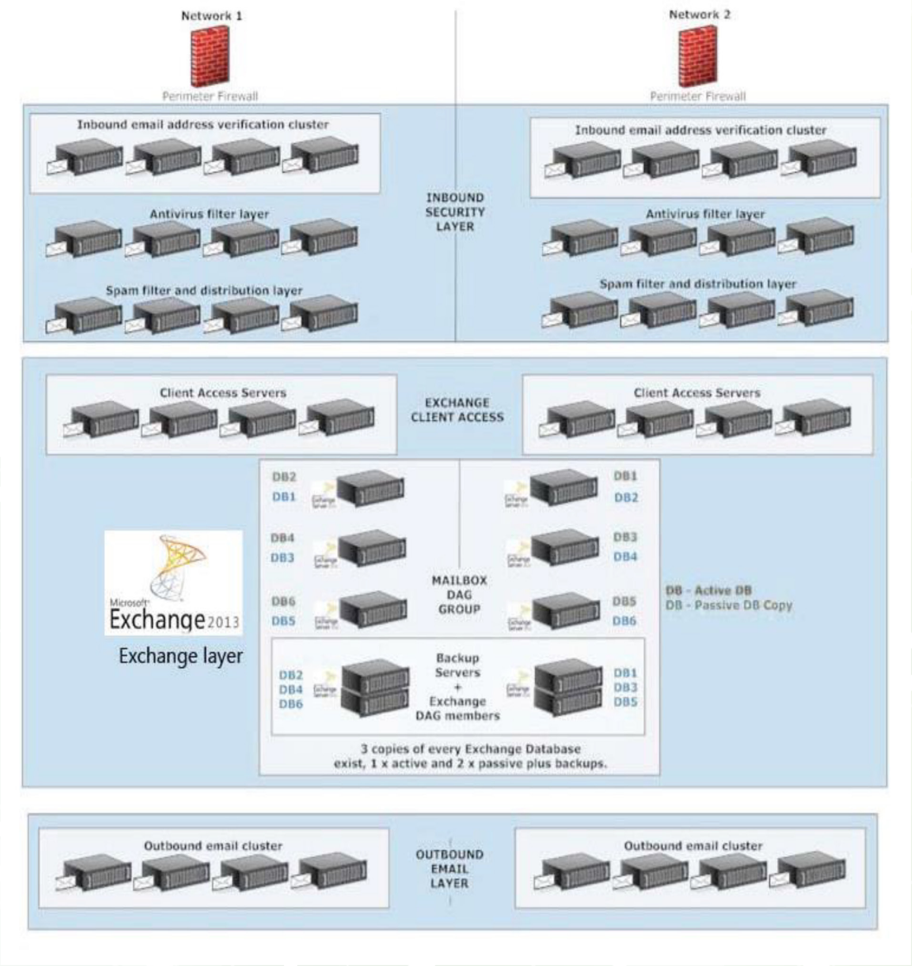
All of our Data Centres are UK based, with multiple based in the North West and multiple in the South.

DATA CENTRE SECURITY

All of our data centres are fully secure locations, with no allowance of any unwanted access. All of the data centres, that we reside are all ISO 27001 certified. All of our data centres work on uninterruptible power, meaning that even with a full power outage, they have on site resources to last a further 7 days. Our data centres offer state-of-the-art fire protection using VESDA systems and FM200 gas suppression. The sites are protected from intruders by a long list of security precautions including secure gated access, the sites are manned 24 hours a day with full protection.

All main and mission critical systems are powered with dual-feeds, this applies globally across all locations.

NETWORK DIAGRAM



HARWARE AND SOFTWARE COVERAGE

We actively hold contracts with all major providers of the equipment we store and house within the Data Centres, these are all contracts holding the most critical support response for all cases, which includes but is not limited to: Barracuda, Cisco, VMWare, Veeam, Microsoft, HP, Dell, and KEMP Load Balancer.

Get in Touch

Tel
0800 019 3878

Email
sales@greencloudhosting.co.uk

Address
Green Cloud Hosting Limited
The Offices,
Barton Arcade,
Deansgate,
Manchester
M3 2BH

Company registration number 7742675
VAT Number 119325032

www.GreenCloudHosting.co.uk

Green Cloud
Hosting™