ukcloud

Pure commitment.

DESIGNING SOLUTIONS FOR HSCN

BLUEPRINT

version 1.0

CONTENTS

OVERVIEW

The HSCN (Health and Social Care Network) is the replacement for the legacy N3 network, which served the health community for 12 years until March 2017 when the contract with BT ends. The N3 was essential for allowing hospitals and GP surgeries to connect and share data, as well as support programmes such as the NHS Care Records service. Now there is a two-year transition period for the NHS to move to HSCN which will last until March 2019.

UKCloud will no longer be offering N3, and will offer HSCN from Q2 onwards.

One of the benefits of HSCN is that there is a lower Information Governance (IG) entry point for connecting to the network. Organisations only need to sign up to the terms detailed in the HSCN Connection Agreement and then they can get access to the HSCN.

.

TIMELINE

Below is a typical example of the standard sequence of events which will be followed by customers and UKCloud in order for them to design and apply for HSCN connectivity;

1. You will usually have a meeting with a UKCloud Cloud Architect in order to start the engagement. The Cloud Architect will be able to understand your requirements and then advise you on best practices around designing for HSCN on UKCloud's Infrastructure as a Service (IaaS) or Platform as a Service (PaaS).

2. You will need to either

    a. Complete the HSCN Connection Agreement, and submit for approval by NHS Digital and then send to UKCloud.

    b. Sign the UKCloud Master Services Agreement (MSA), which includes the flow down of terms from the HSCN Connection Agreement within.

3. A member of the UKCloud Customer Support team will then provision the HSCN-connected environment and hand it over to you once provisioning is complete. You will then be able to build the networks and Virtual Machines (VMs) within the environment, ensuring you continue to follow the best practices for designing for HSCN and do not invalidate the terms of the Connection Agreement.

It should be noted that not all engagements will follow this timeline specifically.

SCENARIOS

There are multiple scenarios that may occur in which you may require HSCN connectivity to provide services in the UK Public Sector. Whilst the following scenarios are not comprehensive, most implementations will follow the same architectural patterns.

Scenario 1: Services connected to HSCN only – Enterprise Compute Cloud (ECC)

All vDCs in Assured ECC environments have an Edge connected to the internet, with HSCN presented as a new Edge. If you are providing services only onto HSCN, you may choose to use only the HSCN Edge and not configure the internet Edge at all. This is rare as most customers will want to be able to automatically pull updates from the internet for VMs. If you choose to only have HSCN configured in your environment then all external source traffic to the VMs within the vDC will originate from the HSCN.

IP Addressing

IP addresses for HSCN are visible on the vCNS Edge device and customers perform firewall configuration on the Edge device to control traffic. You will receive 1 usable HSCN IP as standard, however more can be requested via a service request. If you require a large pool of IPs then it is advisable to request an allocation from NHS Digital directly – UKCloud can then advertise these on your behalf.

Portal Access and VM management

Management of the HSCN connected vDC through the UKCloud Portal and API can be done directly via the internet or HSCN. Remote desktop sessions to manage VMs can only be initiated over the HSCN.
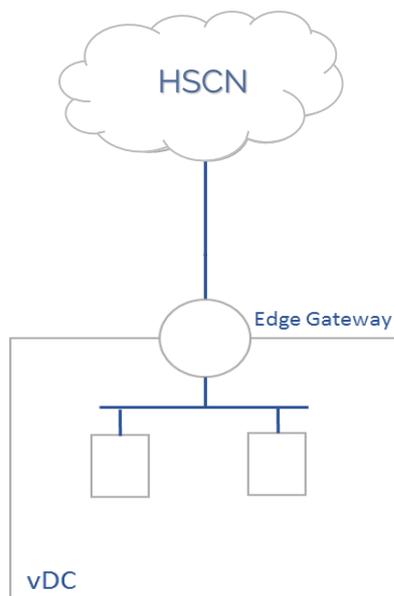

Figure 1. Connection to HSCN only

Scenario 2a: Services connected to HSCN and the Internet – Enterprise Compute Cloud (ECC)

In most scenarios, you will need to provide services out to both the HSCN and internet. When this is configured in ECC, the following architecture explains how the environment should be designed to achieve network separation.
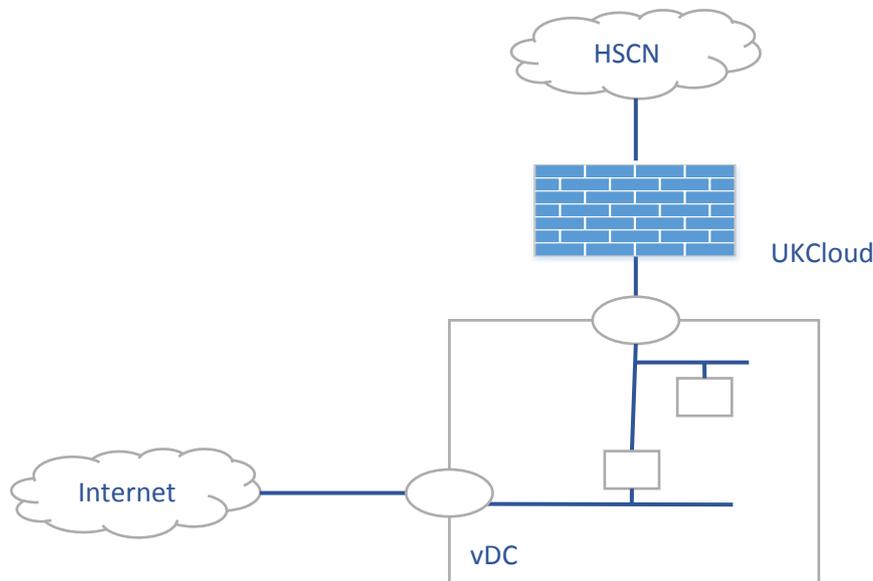

Figure 2. Internet and HSCN using ECC

Networks are separated using different Edge Gateways – firewalling, NAT, External and Internal Network creation are all controlled using both Gateways. vApps can be used to contain VMs that are providing services to the different networks. For more information about VCNS Edge functionality and vApp creation, please see the Getting Started Guide.

Different networks must be used to ensure network separation between N3 and the Internet. In the example in figure 2, the separation of HSCN and Internet is achieved by using an Externally routed network to the internet and a separate Externally routed network to HSCN, which are both connected to a VM. Network separation is achieved through firewalls. You must not join an Externally routed network to both HSCN and internet at the same time.

IP Addressing

IP addresses for HSCN are visible on the vCNS Edge device and customers perform firewall configuration on the Edge device to control traffic. You will receive 1 usable HSCN IP as standard, however more can be requested via a service request. If a customer requires a large pool of IPs then it is advisable to request an allocation from NHS Digital directly – UKCloud can then advertise these on your environment.

You will also receive 2 internet IPs per vDC.

Portal Access and VM management

Management of the vDCs through the UKCloud Portal and API can be done via the internet and HSCN. Remote desktop sessions to manage HSCN connected VMs can be initiated

over the HSCN or over the internet by using a jump-off server within the internet facing part of the environment.

Scenario 2b: Services connected to HSCN and the Internet – Cloud Native Infrastructure (CNI)

When designing a HSCN-connected cloud native solution, it's important to ensure network separation to prevent bridging between HSCN and the internet. This can be done by using a series of networks and instances to build your solution, **ensuring that there is not a single network spanning between both HSCN and internet routers.**

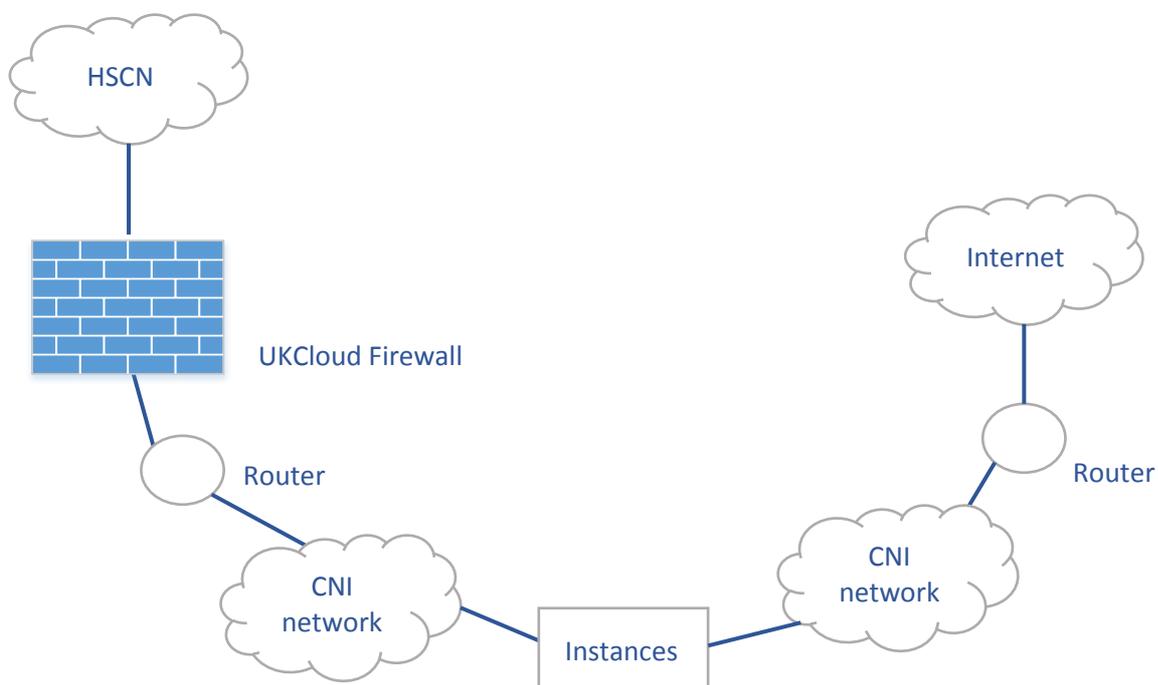Figure 3 shows what a typical CNI implementation should look like to achieve network separation.

Figure 3. Internet and HSCN using CNI

IP Addressing

Your assigned floating HSCN IP address will be visible within your CNI project; you can then create routers to present that IP to the rest of your environment. The UKCloud controlled firewall permits HSCN traffic on standard ports – you will need to provision your own firewalls to control traffic. You will receive 1 usable HSCN IP as standard, however more can be requested via a service request. If you require a large pool of IPs then it is advisable to request an allocation from NHS Digital directly – UKCloud can then advertise these on your environment.

You will receive 2 internet IPs per project and will need to provision another firewall for the internet.

Portal Access and VM management

Management of Projects through the UKCloud Portal and API can currently only be done directly via the internet. Remote desktop sessions to manage HSCN connected instances can be initiated over the HSCN or over the internet by using a jump-off server within the internet facing part of the environment. **For you to be able to manage the environment over HSCN, you must create an RDP session to an instance within the project and then hit the portal from within the project itself.**

Scenario 3: Services built on Internet vDC and HSCN connectivity added post-build

You may start creating services and then add HSCN later. In this instance, the environment would have connectivity to only the internet. When you have signed up to the terms of the Connection Agreement and are ready for HSCN, you would need to raise a service request for HSCN connectivity to be added to the environment; this will be added as a second Edge Gateway.

Scenario 4: HSCN connected vDC with services in the Elevated platform

HSCN connectivity is currently only available into UKCloud's Assured platform. There may be scenarios where you are providing services over HSCN, but the data itself is deemed too sensitive to be stored in the Assured platform. Therefore you may wish to have a vDC in the Elevated platform to host the data into, to ensure there is separation between the internet/HSCN facing services and the database.

In order to move data from the Assured (HSCN facing) vDC into the Elevated platform, the Cross Domain Security Zone (CDSZ) must be used to ensure the integrity of the data in the Elevated platform. For more information on the CDSZ, please see the Service Description, Blueprint and application form available in the Knowledge Centre.
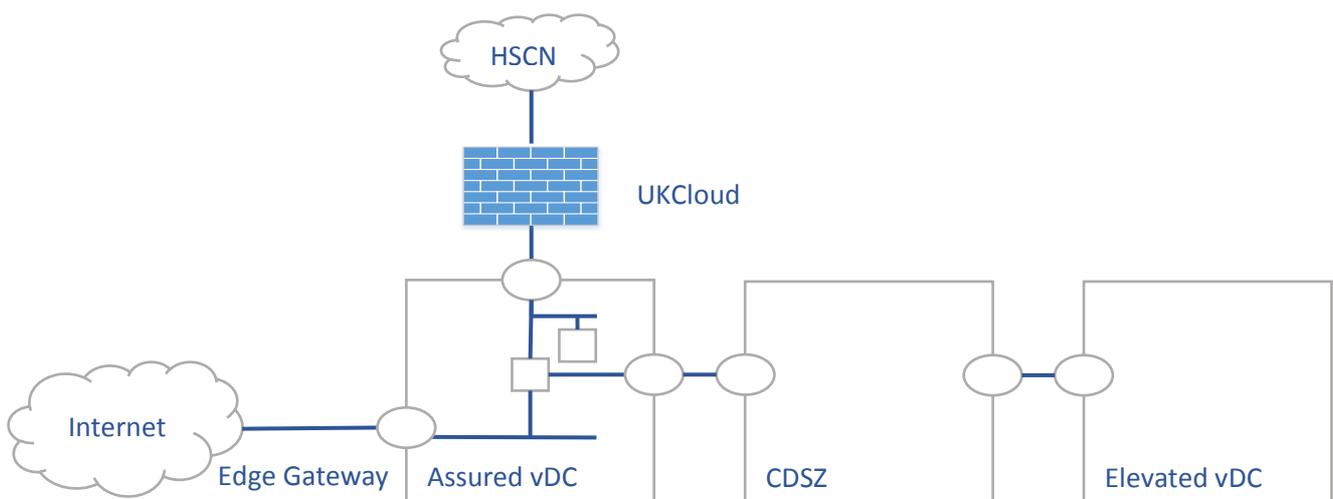

Figure 4. Cross Domain Security Zone

You can have a VM that is connected to three Externally routed networks – one to HSCN, internet and the CDSZ network.

In some cases, you may need to provide a service both to the HSCN and to the PSN-P at the same time. In order to facilitate this, you would need to use the CDSZ in order to traverse between the HSCN connected Assured platform and the PSN-P connected Elevated platform. The architecture will allow onward PSN-P connectivity for services in the Elevated vDC. In order for PSN-P connectivity to be allowed, you must have a PSN Code of Connection or Code of Practice which they must present to UKCloud.
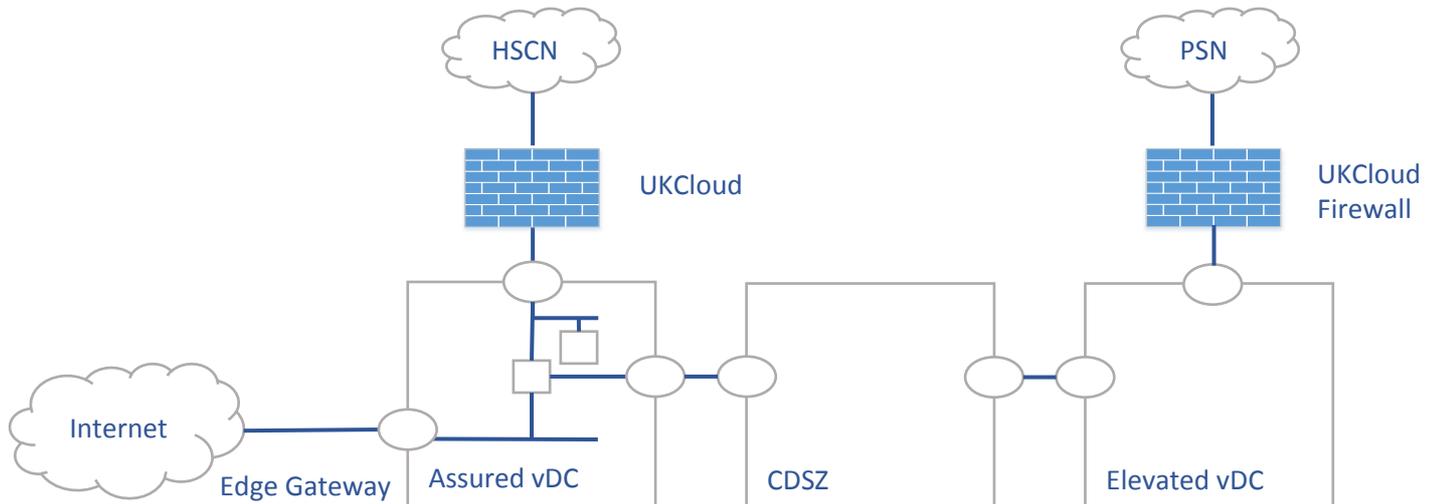

Figure 3. Cross Domain Security Zone and PSN-P

IP Addressing

IP addresses for HSCN are visible on the vCNS Edge device and you can perform firewall configuration on the Edge device to control traffic. You will receive 1 usable HSCN IP as standard, however more can be requested via a service request. If you require a large pool of IPs then it is advisable to request an allocation from NHS Digital directly – UKCloud can then advertise these on your environment.

You will receive 2 internet IPs per vDC. You will be able to perform NAT functions on the Edge to ensure internet connectivity for VMs within the environment.

PSN-P connectivity is provided to the Elevated vDC through a UKCloud controlled firewall. The PSN-P address is translated at this firewall to an internal address and is routed to the Edge on the Elevated vDC. There are 5 IPs that are connected to the Elevated vDC Edge. You can specify which one of these addresses they would like the PSN-P IP translated to.

Portal Access and VM management

Management of the Assured (internet/HSCN connected) vDC through the UKCloud Portal and API can be done via the internet and HSCN. Remote desktop sessions to manage HSCN connected VMs can be initiated over the HSCN or over the internet by using a jump-off server within the internet facing part of the environment.

Management of the Elevated (PSN-P connected) and CDSZ vDCs through the UKCloud Portal and API can currently only be done via the PSN-P or by using UKCloud's Secure

Remote Access (SRA) service. For more information on SRA, please see the [SRA Service Description](#) available in the Knowledge Centre.

Additional Information

Getting OS updates to servers that are on the HSCN

There is currently no direct connectivity between VMs that are connected to the HSCN and the Operating System (OS) repositories that are provided by UKCloud.

For HSCN connected VMs to receive updates, a repository server must be provisioned within the HSCN facing environment. This VM should be provisioned with connectivity to both external public IP networks and an internal network connected to VMs with onward connectivity to the HSCN. Relevant OS updates should be downloaded to this server and distributed to the other VMs within the vDC to ensure they remain up-to-date with patches.

Opening ports on HSCN

UKCloud has a list of whitelisted ports that are open as standard on our firewalls. This [list](#) is available within our Knowledge Centre. If you require additional ports to be opened for HSCN then they can do so by raising a service request.

Adding HSCN to an existing vDC

If you have deployed your vDC and later wish to connect it to HSCN then this can be done by signing up to the HSCN Connection Agreement terms. A new Edge with HSCN will then be provisioned into the environment.

ABOUT UKCLOUD

UKCloud is dedicated to the UK Public Sector. We provide assured, agile and value-based true public cloud that enable you to deliver enhanced performance through technology.

- **We're focused on cloud.** Delivering a true cloud platform that is scalable, flexible, assured and cost-effective.

- **We're open. You are never locked in.** Using industry standards and open source software we enable flexibility and choice across multiple cloud solutions.

- **Dedicated to the UK Public Sector.** Our business is designed specifically to serve and understand the needs of public sector organisations. **develop communities.** We bring together communities of users that are able to share datasets, reuse code, test ideas and solve problems.

- **Customer engagement.** We will only be successful if our customers are successful. We embody this in the promise: Easy to adopt. Easy to use. Easy to leave.

Additional information about UKCloud can be found at www.ukcloud.com or by following us on Twitter at @ukcloudltd.

UKCloud. The power behind public sector technology.

MORE INFORMATION

For further information about UKCloud and how we can help you, please email us at info@ukcloud.com.