Azure Secure Environment

Build Document

October 2017

Revised July 2018 – Document anonymised

Prepared by

Contents

Overview 4
Virtual Network Configuration 4
Topology Overview 5
Prerequisites 6
Installation Order 6
Azure Configuration 7
Overview 7
Virtual Network 7
Azure AD 7
MFA Configuration 7
Domain Controller 8
General VM specification 8
Windows Configuration 8
Active Directory Configuration 8
Group Policy Configuration 9
Windows Update Service Configuration 13
Azure AD Connect 14
RDS Session Servers (x2) 15
General VM specification 15
Azure Configuration 15
Windows Configuration 15
Additional Apps 15
RDS Server 16
General VM specification 16
Azure Configuration 16
Windows Configuration 16
RDS Installation 17
RDS Configuration 17
Public Domain Configuration 18
Network Policy Server 19
General VM specification 19
Windows Configuration 19
Azure Configuration 19
Network Policy Configuration 19
SQL Server Installation 19
Data Server 20
General VM specification 20
Windows Configuration 20

GitLab Server 21
General VM specification 21
Azure Configuration 21
Ubuntu Configuration 21
GitLab Configuration 21
Jupyter Lab Server 22
General VM specification 22
Azure Configuration 22
Ubuntu Configuration 22
HackMD 24
Network Security Groups 25
Operation Management Suite 25
Azure Extension Installation 25
Azure Recovery Services 26
Azure Disk Encryption 26

Overview

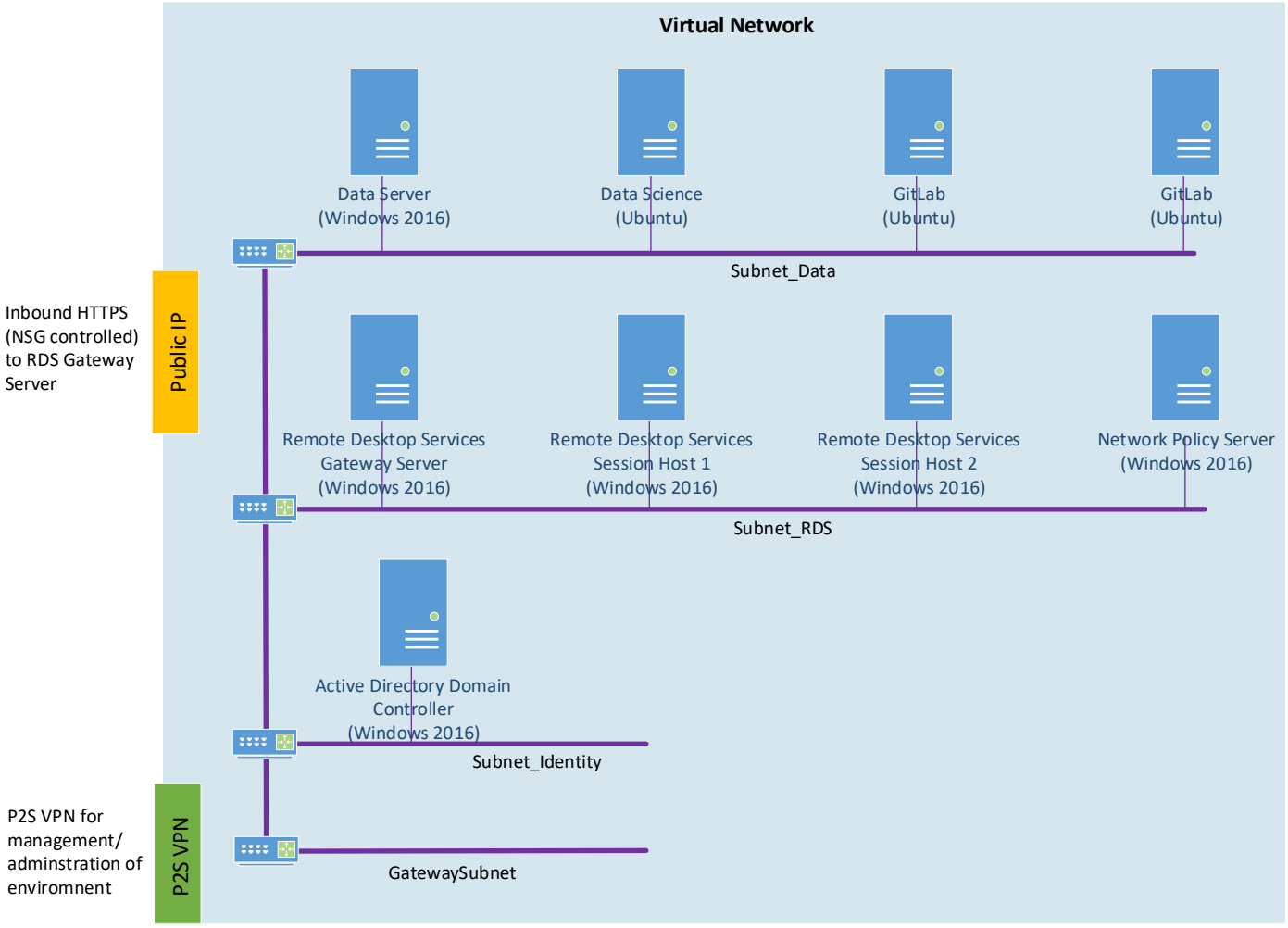
The environment is built within a single Azure virtual network and has the following conditions:

- All servers isolated from inbound connections from the internet except the RDS Gateway Server
- Single point of entry via Windows Remote Desktop Services from known IP range
- Single identity provider to control access to servers, data and apps (Active Directory)
- 2 factor authentications to access RDS system
- SSL encrypted communications
- Data cannot be moved/copied from the environment
- Data science development tools available
- Audit logging to monitor authentication requests and system changes
- Windows updates enabled

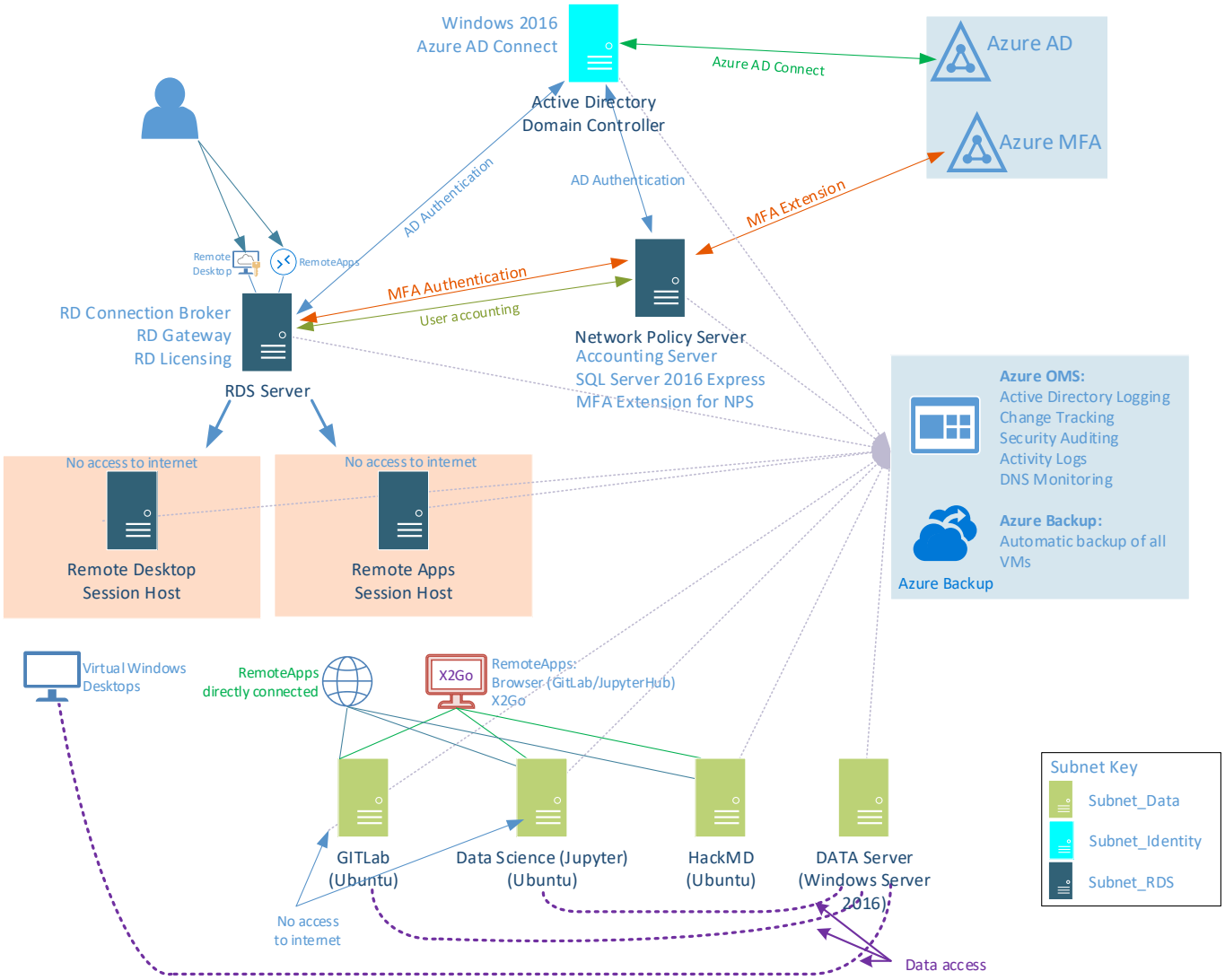
The majority of the infrastructure is built using PowerShell scripts within Microsoft Azure. Linux servers once provisioned require further OS updates and additional packages installed.

Knowledge of both Windows Server and supported services, Microsoft Azure and Linux along with development environments is assumed.

Virtual Network Configuration



Topology Overview



Prerequisites

The secure environment requires the following elements to be successfully deployed

- Public domain name registered with an internet registrar
- Public CA SSL certificate, used for RDS services
- Azure subscription
- Azure AD Premium 2 subscription associated with the above new subscription.

Installation Order

For a successful installation the servers are required to be configured in the following order:

Domain Controller -> RDS Session Hosts – RDS Server -> NPS Server -> Data Server -> Linux Servers

Azure Configuration

Overview

The Azure configuration requires the following:

- Subscription that is funded from the Microsoft research sponsorship
- An additional Azure subscription that is used for the Azure AD and Azure MFA component

Virtual Network

Virtual network created with the following attributes:

- Class A address 0.0.0.0/00
- Subnets:
    - Subnet_Data – 0.0.0.0/00
    - Subnet_Identity – 0.0.0.0/00
    - Subnet_RDS – 0.0.0.0/00
-
- Point to Site VPN
    - GatewaySubnet - 0.0.0.0/00

Azure AD

To ensure that the user I'd are contained with a separate AAD it is advisable to setup a new trial Azure subscription. In addition to the trail subscription the following is required:

- Azure AD Premium Trail
- Add custom domain (i.e. dsgroup1.co.uk) and make primary
- MFA enabled
- Password write back enabled
- Password self-service reset enabled
- Service account created for Azure AD management, this account is used by MFA and Azure AD Connect

MFA Configuration

- Do not allow users to create app passwords
- Verification options:
    - Call to phone
    - Notification through mobile app

Domain Controller

General VM specification

- Admin user ID = <Admin User Name>
- Windows Server 2016
- VM Size D2v2
- Static internal IP address
- No public IP address
- Additional 20Gb data disk for AD Databases (Disk caching disabled)
- Additional 256Gb data disk for WSUS data files

Windows Configuration

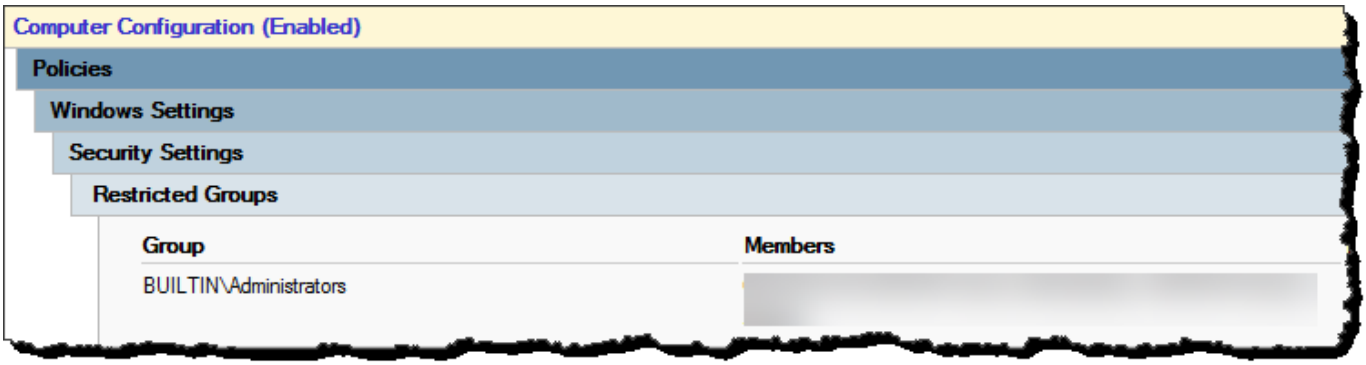
- Name: <VM Name>
- Server language, region to UK
- Time zone set to GMT
- Active Directory Domain Services installed
    - Forest name = publicdomainname.co.uk
    - Functional level = Windows Server 2016
    - AD databases and SYSVOL created on additional 20Gb drive
- Windows Update Services installed
    - WSUS database/files stored on 256Gb disk

Active Directory Configuration

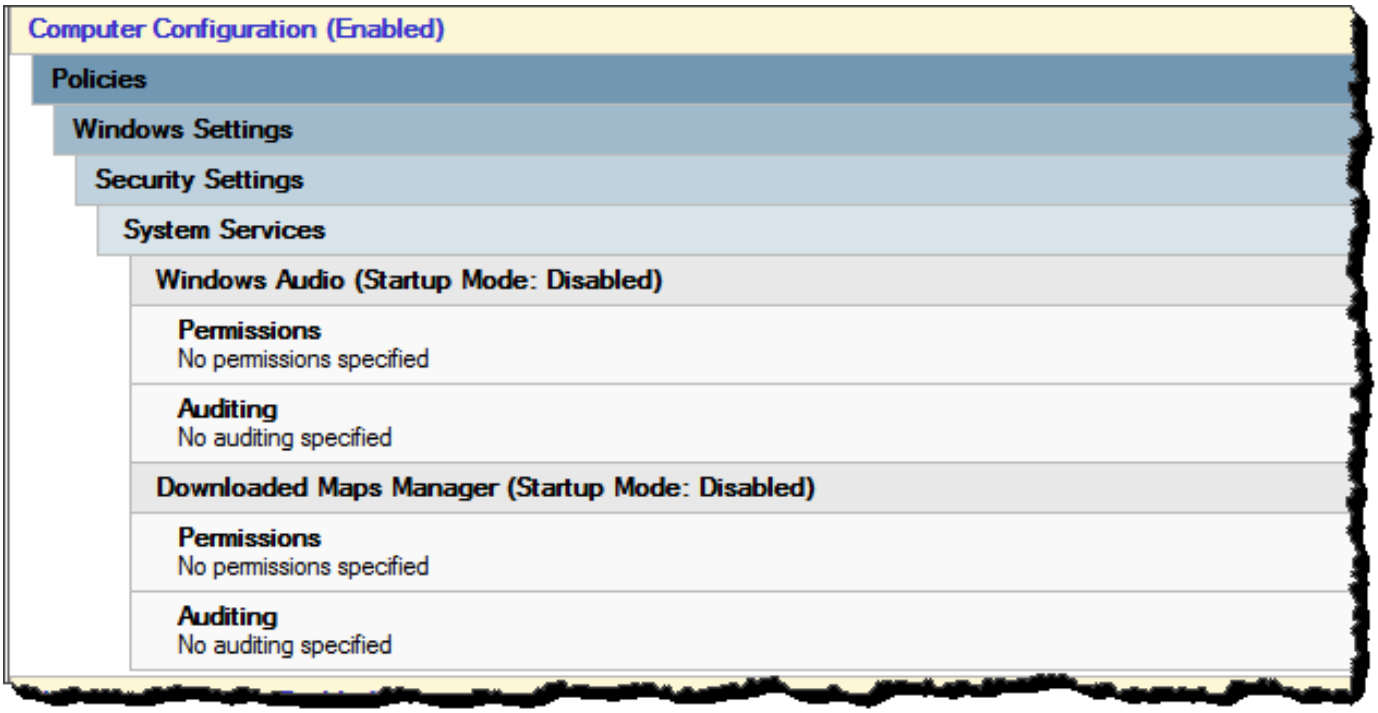
- Set “<Admin User Name>” account password to “Never Expire”
- Security Groups:
    - Data Servers
    - RDS Session Servers
    - Research Users
    - Security Groups
    - Service Accounts
    - Service Servers
- Service Accounts
    - GitLab server LADP lookup (used for GitLab LDAP lookup)
    - Local AD Sync Admin (used for AD Connect) must be member of enterprise admins (created by AAD Connect software)
    - SQL Server Service Account (used by SQL server on NPS server)
- Security Groups
    - SG Research Users
        - All research users
    - SG Server Administrators
        - Users who need admin access to servers (IT team)
- Configure DNS
    - Create Reverse lookup zones
    - Add GITLab, Data Science, HackMD to DNS

Group Policy Configuration

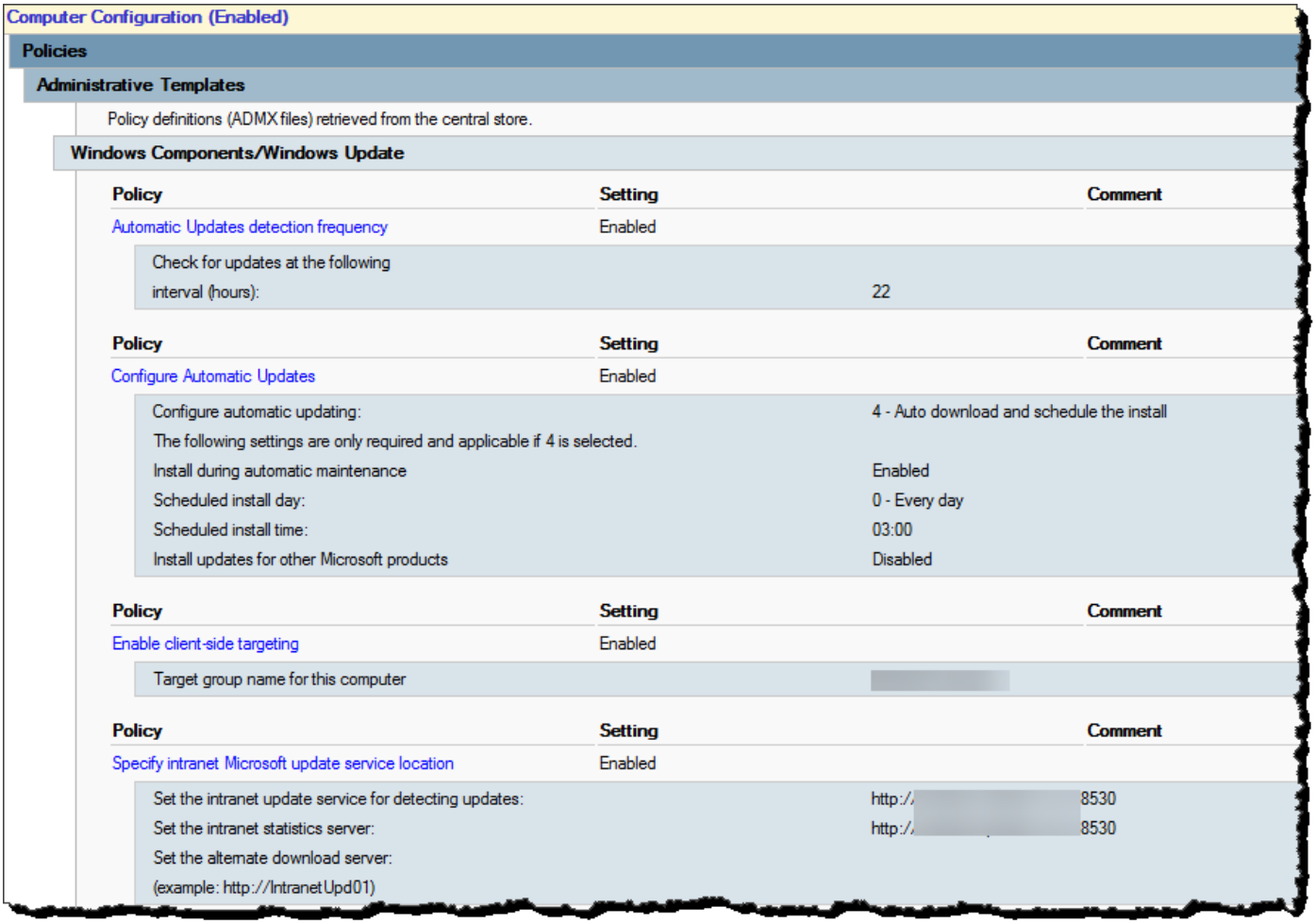
GPO Name: All servers – Local Administrators
Applied to: Data Servers, RDS Session Servers, Service Servers



GPO Name: All Servers – Windows Services
Applied to: Domain Controllers, Data Servers, RDS Session Servers, Service Servers



GPO Name: All Servers – Windows Update
Applied to: Domain Controllers, Data Servers, RDS Session Servers, Service Servers



Computer Configuration (Enabled)

Policies

Administrative Templates

Policy definitions (ADMX files) retrieved from the central store.

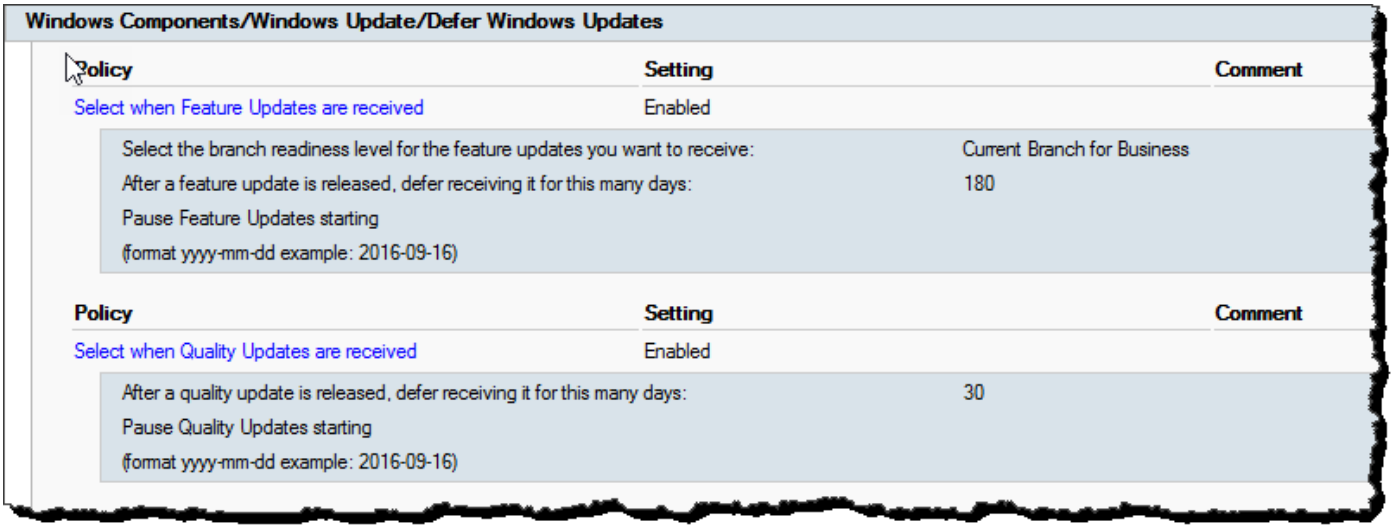
Windows Components/Windows Update

Policy	Setting	Comment
Automatic Updates detection frequency	Enabled	
Check for updates at the following interval (hours):	22	

Policy	Setting	Comment
Configure Automatic Updates	Enabled	
Configure automatic updating:	4 - Auto download and schedule the install	
The following settings are only required and applicable if 4 is selected.		
Install during automatic maintenance	Enabled	
Scheduled install day:	0 - Every day	
Scheduled install time:	03:00	
Install updates for other Microsoft products	Disabled	

Policy	Setting	Comment
Enable client-side targeting	Enabled	
Target group name for this computer	[redacted]	

Policy	Setting	Comment
Specify intranet Microsoft update service location	Enabled	
Set the intranet update service for detecting updates:	http://[redacted]:8530	
Set the intranet statistics server:	http://[redacted]:8530	
Set the alternate download server: (example: http://IntranetUpd01)		

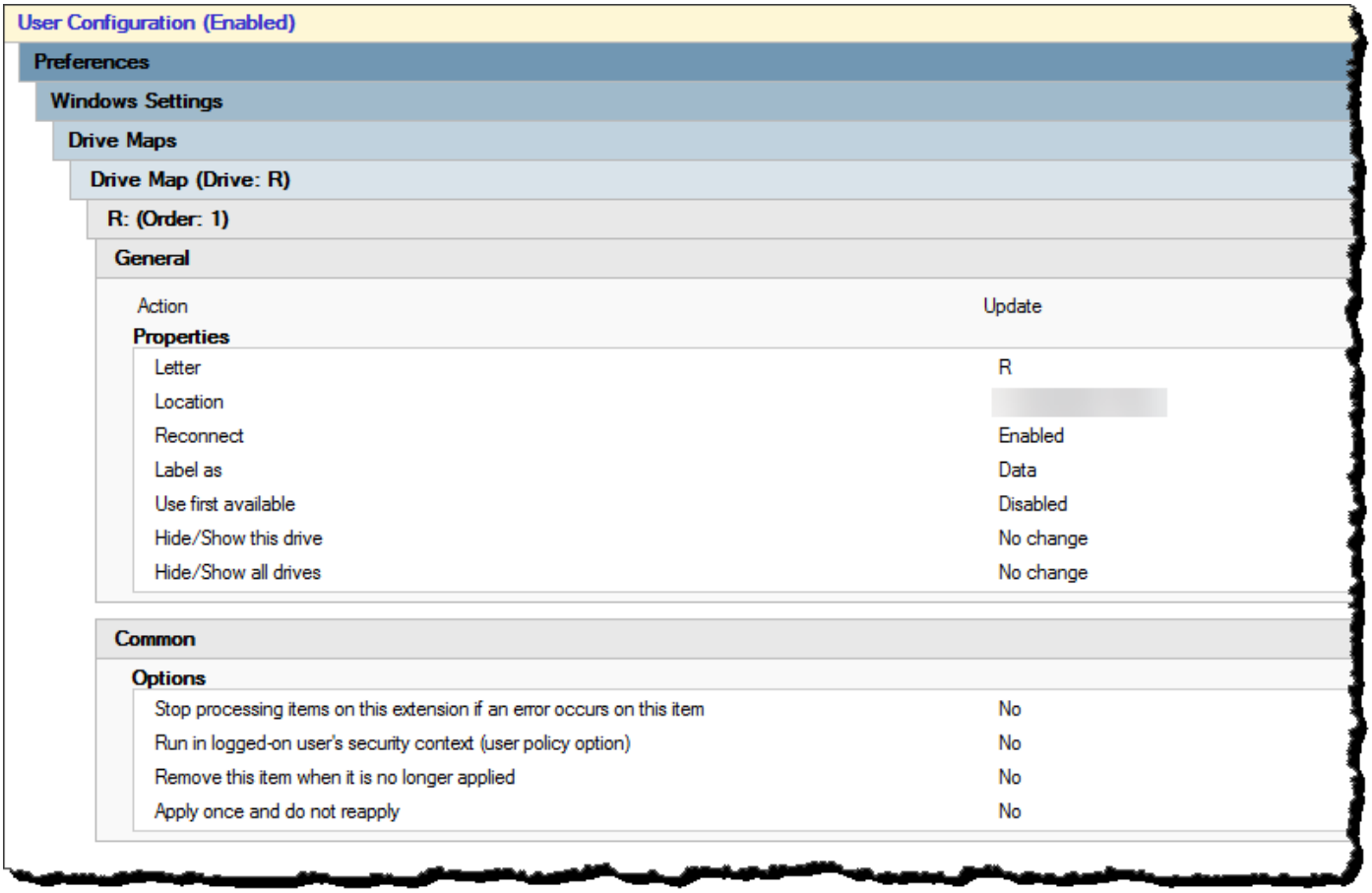


Windows Components/Windows Update/Defer Windows Updates

Policy	Setting	Comment
Select when Feature Updates are received	Enabled	
Select the branch readiness level for the feature updates you want to receive:	Current Branch for Business	
After a feature update is released, defer receiving it for this many days:	180	
Pause Feature Updates starting (format yyyy-mm-dd example: 2016-09-16)		

Policy	Setting	Comment
Select when Quality Updates are received	Enabled	
After a quality update is released, defer receiving it for this many days:	30	
Pause Quality Updates starting (format yyyy-mm-dd example: 2016-09-16)		

GPO Name: Research Users – Mapped Drives
Applied to: Research Users



User Configuration (Enabled)

Preferences

Windows Settings

Drive Maps

Drive Map (Drive: R)

R: (Order: 1)

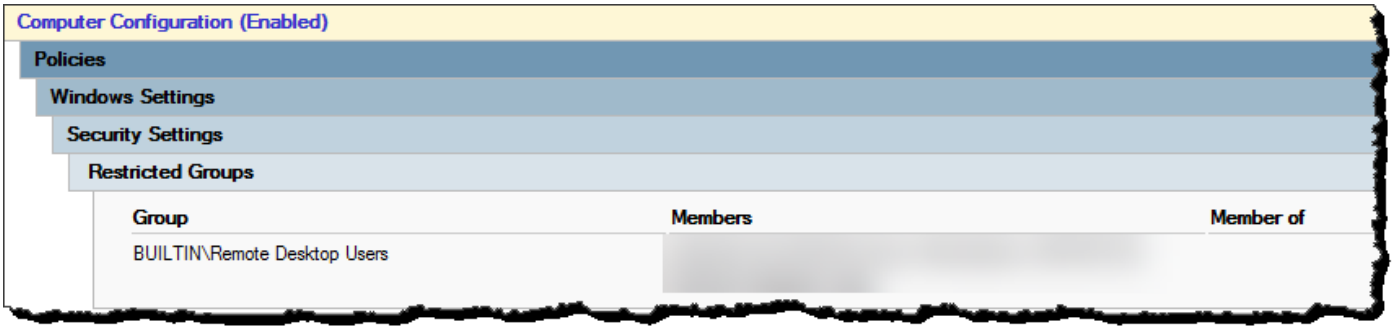
General

Action	Update
Properties	
Letter	R
Location	
Reconnect	Enabled
Label as	Data
Use first available	Disabled
Hide/Show this drive	No change
Hide/Show all drives	No change

Common

Options	
Stop processing items on this extension if an error occurs on this item	No
Run in logged-on user's security context (user policy option)	No
Remove this item when it is no longer applied	No
Apply once and do not reapply	No

GPO Name: Session Servers – Remote Desktop Control
Applied to: RDS Session Servers, Research Users



Computer Configuration (Enabled)

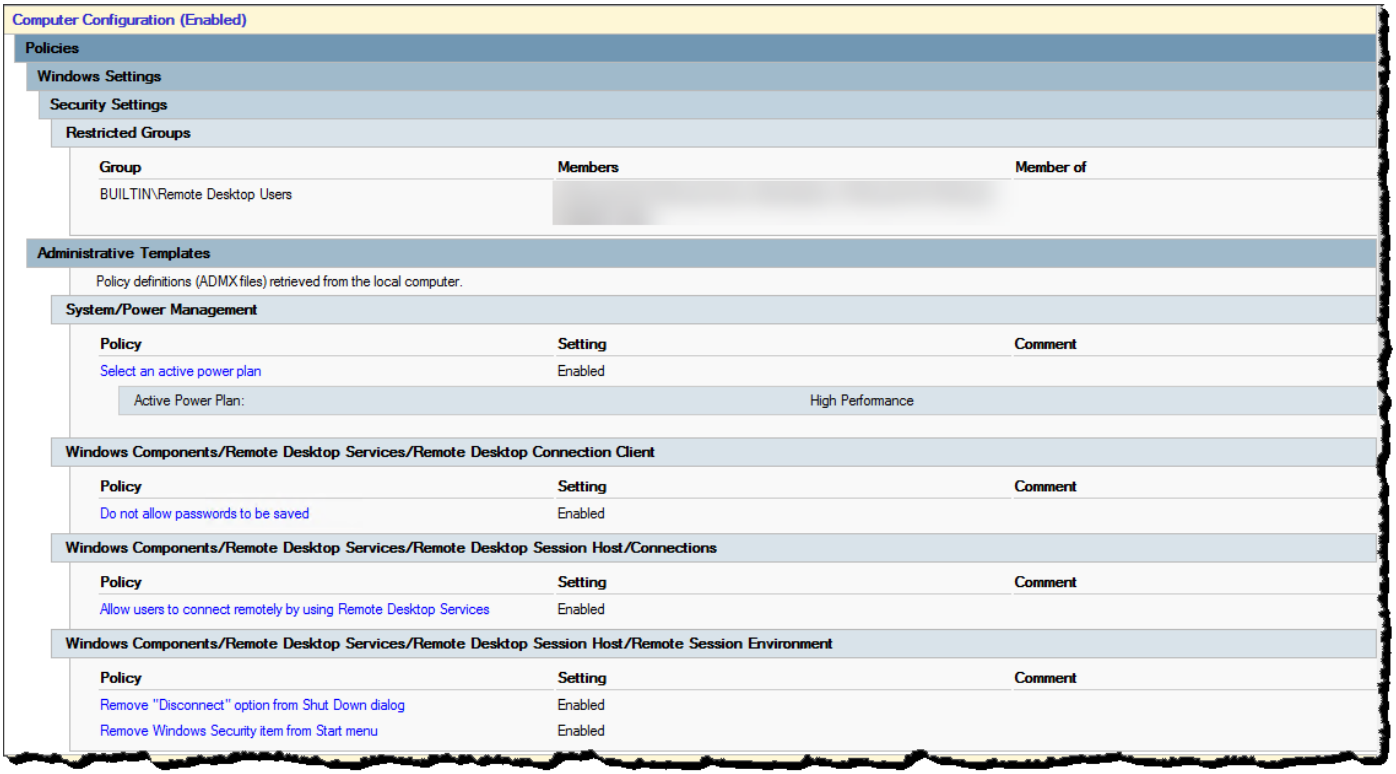
Policies

Windows Settings

Security Settings

Restricted Groups

Group	Members	Member of
BUILTIN\Remote Desktop Users		



Computer Configuration (Enabled)

Policies

Windows Settings

Security Settings

Restricted Groups

Group	Members	Member of
BUILTIN\Remote Desktop Users		

Administrative Templates

Policy definitions (ADMX files) retrieved from the local computer.

System/Power Management

Policy	Setting	Comment
Select an active power plan	Enabled	
Active Power Plan:	High Performance	

Windows Components/Remote Desktop Services/Remote Desktop Connection Client

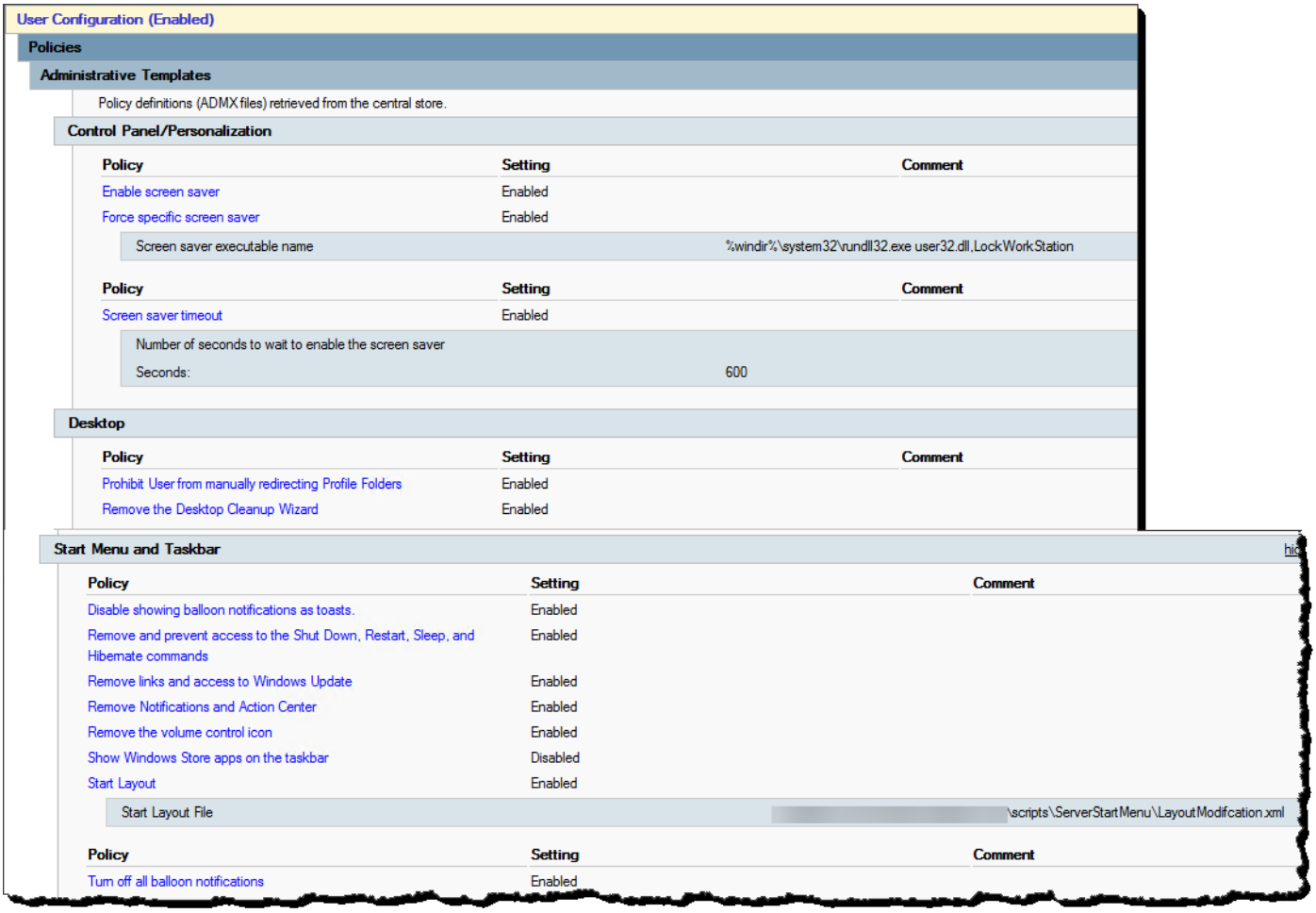
Policy	Setting	Comment
Do not allow passwords to be saved	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Connections

Policy	Setting	Comment
Allow users to connect remotely by using Remote Desktop Services	Enabled	

Windows Components/Remote Desktop Services/Remote Desktop Session Host/Remote Session Environment

Policy	Setting	Comment
Remove "Disconnect" option from Shut Down dialog	Enabled	
Remove Windows Security item from Start menu	Enabled	



Screensaver exe path: %windir%\system32\rundll32.exe user32.dll,LockWorkStation
LayoutModification.xml file stored in SYSVOL\domain\scripts\ServerStartMenu

LayoutModifcation.xml

Windows Update Service Configuration

- Database and files stored on 256Gb Drive
- Products:
  - Windows Defender
  - Windows Server 2016
- Classifications:
  - Critical Updates
  - Definition Updates
  - Security Updates
- Automatic approval enabled for all updates (Critical, Definition, Security)
- Use Group Policy on computers
- New group created: Name to match the one set in GPO for windows update

Azure AD Connect

- Azure AD Connect installed and connected to new Azure AD subscription
    - Custom Install
    - Password synchronisation
    - Sync only “Research Users” OU
    - Password write back enabled

RDS Session Servers (x2)

General VM specification

- Admin user ID = <Admin User Name>
- Windows Server 2016
- VM Size D11v2
- Static internal IP address
- No Public address

Azure Configuration

- NSG configured to prevent internet access but allow access to Azure services

Windows Configuration

- Name: SERVER 1, SERVER 2
- Server language, region to UK
- Time zone set to GMT
- Domain joined
- OU = Session Hosts
- Latest Windows updates applied

Additional Apps

- Install Chrome and X20Go client and add icons to the default user profile “Desktop”

RDS Server

General VM specification

- Admin user ID = <Admin User Name>
- Windows Server 2016
- VM Size D11v2
- Static internal IP address
- Static Public address
- 2x Additional 1Tb disks

Azure Configuration

- Network Security Group
    - HTTPS Inbound

Windows Configuration

- Name: SERVER NAME
- Server language, region to UK
- Time zone set to GMT
- Domain joined
- OU = Service Servers
- Latest Windows updates applied
- Public CA Certificate installed (match name of server)
- Remote App File Share:
    - Drive: E:\
    - Volume Name: App File Shares
    - Folder name: AppFileShares
    - Sharename: AppFileShares
    - Permissions:
        - Domain admin: FC
        - Computer account for SERVERNAME: FC
        - Everyone: Removed
- Remote Desktop File Share:
    - Drive: F:\
    - Volume Name: RDP File Shares
    - Folder name: RDPFileShares
    - Sharename: RDPFileShares
    - Permissions:
        - Domain admin: FC
        - Computer account for SERVERNAME: FC
        - Everyone: Removed

RDS Installation

- Standard Deployment
- Session based deployment
- Use current server for RD Connection broker
- Use current server for Web Access
- Add Session host servers (these need to be domain joined and added to Server Manager console before this can be completed)
- Configure RDS licensing server
    - Specify local server as RDS license server
    - Licensing model: Per Device
    - SSL certificate installed onto licensing server
    - Activate RDS licensing server

RDS Configuration

- Create Remote Application collections
    - Collection Name: Remote Applications
    - User Groups: SG Research Users
    - User Profile Disks:
        - Enabled
        - Location: \\SERVERNAME\AppFileShares
        - Size: 50Gb

- Configure Collection:
    - Session: Defaults
    - Security:
        - General: As configured above
        - User Groups: As configured above
        - Security Layer: Negotiate
        - Encryption Level: Client Compatible
        - Load Balancing: Default
        - Client Settings: All redirection properties disabled
        - Store only the following:
            - Desktop
            - Documents
            - Download
            - Roaming user profile data
            - User registry data

- Create remote apps
    - GitLab
        - Browser (Chrome) connection to GitLab server web interface http://0.0.0.0
    - Jupyter Hub
        - Browser (Chrome) connection to Jupyter hub web interface https://0.0.0.0:8000
    - X2Go Client

- Configure Virtual Desktop Sessions

    - Collection Name: Remote Desktop
    - User Groups: SG Research Users
    - User Profile Disks: Enabled
        - Location: \\SERVERNAME\RDPFileShares
        - Size: 50Gb

- Configure Collection:
    - Session: Defaults
    - Security:
        - General: As configured above
        - User Groups: As configured above
        - Security Layer: Negotiate
        - Encryption Level: Client Compatible
        - Load Balancing: Default
        - Client Settings: All redirection properties disabled
        - Store only the following:
            - Desktop
            - Documents
            - Download
            - Roaming user profile data
            - User registry data

Public Domain Configuration

- A record created in the public DNS for the RDS server i.e. rds.DOMAIN.co.uk

Network Policy Server

General VM specification

- Admin user ID = <Admin User Name>
- Windows Server 2016
- VM Size D2v2
- Static internal IP address
- No public IP address
- Additional 128Gb data disk for SQL Databases (Disk caching disabled)

Windows Configuration

- Server language, region to UK
- Time zone set to GMT
- Domain joined
- OU = Service Servers
- Latest Windows updates applied

Azure Configuration

- Service account is created within the AAD
- Azure AD Premium is enable on the AAD
- Custom Domain is verified and made primary on AAD

Network Policy Configuration

- Install Visual C++ 2013 Redistributable
- Install MSOnline PowerShell for Azure Active Directory v1.1.1166+
- Install Network Policy and Access Services role with default settings
- Configure NPS and MFA extension – Microsoft Document
    - User ACCOUNTNAME@domain.onmicrosoft.com as the AAD login

SQL Server Installation

- SQL Server 2017 Express install inc. management studio
- Default instance (MSSQLServer)
- SQL Engine user – SQL ADMIN USER
- Data and log files to be stored on 128G disk (E:)
- SQL service account used for database engine and agent user
- Set Max memory to 1024Mb
- Create database called “UserAccounting”
- Enable TCP/IP network protocol
- Add firewall rules to allow 1433
- Configure user accounting in NPS to log to the SQL server

Data Server

General VM specification

- Admin user ID = <Admin User Name>
- Windows Server 2016
- VM Size D2v2
- Static internal IP address
- No Public address
- Additional 512Gb data disk for data

Windows Configuration

- Name: SERVERNAME
- Server language, region to UK
- Time zone set to GMT
- Domain joined
- OU = Data Servers
- Latest Windows updates applied
- Share created on 512Gb data disk called “Data” and shared to the “Research Users” security group with change rights. Add domain admins and SG Server Administrators with FC to the same share

GitLab Server

General VM specification

- Admin user ID = <Admin User Name>
- Gitlab Community Edition
- VM Size D2v2
- Static internal IP address
- No Public address
- Data Disk size set to 750Gb

Azure Configuration

- NSG configured to prevent internet access but allow access to Azure services

Ubuntu Configuration

- Host files updated with host name and IP address
- Data disk formatted and mounted (mount on reboot)
- Create directory on new data drive to be used for GitLab home data
- Change region and time zone to UK/GMT
- Install AuditD (required for OMS agent)

GitLab Configuration

- Update GitLab LDAP configuration to connect to AD domain and DC
- Update GitLab configuration to change default data directory to newly created directory on the data disk
- Update GitLab settings and disable “Sign-up” option
- Test login to GitLab with a domain user

  GitLab Reference - https://docs.gitlab.com/ee/administration/auth/ldap.html#enabling-ldap-sign-in-for-existing-gitlab-users

- Upgrade GitLab to v10.x

Jupyter Lab Server

General VM specification

- Admin user ID = <Admin User Name>
- Data Science Ubuntu
- VM Size NC12
- Static internal IP address
- No Public address
- OS Disk size set to 100Gb

Azure Configuration

- NSG configured to prevent internet access but allow access to Azure services

Ubuntu Configuration

- Update the host file with the host name and IP address
- Change region and time zone to UK/GMT
- Configure Ubuntu for Kerberos/LDAP integration
- Install AuditD (required for OMS agent)
- Join the server to the AD
- Configure Pam.d to create home directory to match users domain name on login
- Upgrade/update Ubuntu to latest patch level
- Update X2Go server
- Install Conda Packages

python3-dev	spacy	cython
nose	wordcloud	pyLDAvis
nltk	tqdm	libudunits2-dev
plotly	GPy	libapparmor-dev
Lifelines	nomkl	libgdal1-dev
pandas-profiling	numpy	jags
geohash2	setuptools	r-cran-slam
pymc3	dash	gdal-bin
pystan	edward	libgsl-dev
CVXPY	glove_python	libpoppler-cpp-dev
scipy	scikit-learn	libgdal1i
rpy2	gmplot	libproj-dev
dash-renderer	dash-html-components	r-cran-rjava
tensorflow-gpu	textblob	r-cran-spatstat
Mne	dash-core-components	libgsl2
libv8-3.14-dev	PyTorch	

- Upgrade Python3
- Install R Packages:

abind	akima	dygraphs
ape	caret	keras
cluster	coda	PtProcess
corrplot	cowplot	stlplus
cvTools	data.table	VGAM
devtools	directlabels	bsts
dlm	doBy	hawkes
dplyr	emulator	cbreto/panelPomp
fields	fiftystater	timeSeries
forecast	gamlss	tseries
gamlss.dist	gamlss.mx	ranger
gamlss.nl	gamlss.spatial	rminer
geohash	ggforce	RRF
ggmap	ggplot2	acp
ggridges	gplots	brms
gridExtra	kernlab	glarma
knitr	LDAvis	plotly
lme4	lubridate	ppmlasso
magrittr	maps	tscount
MASS	McSpatial	wavelets
mlbench	mlr	dplR
nlme	pomp	IHSEP
pscl	quanteda	RHawkes
Raster	readr	quantmod
RColorBrewer	readtext	cleanNLP
revealjs	reshape2	verification
rgdal	rgeos	widyr
rPython	rstan	topicmodels
runjags	RWeka	vars
Scale	scales	wordcloud
slam	SnowballC	dummies
sp	spacyr	tmap
stargazer	stm	urca
stringr	surveillance	viridis
text2vec	tidyr	Xlsx
tidytext	tidyverse	BayesianTools
dtw		

- Update R to use new IRKernel (fixes error shown in Jupyter)
- Expand the data drive to 750Gb

HackMD

NOTE: Users must have an email address specified in their Active Directory profile i.e. username@DOMAIN.co.uk. This is used only for the HackMD LDAP implementation that will throw a login error if this field is empty

- Update the host file with the host name and IP address
- Change region and time zone to UK/GMT
- Install AuditD (required for OMS agent)
- Update OS/patch level to latest
- Install Docker
- Clone Docker-hackmd from Github
- Configure Docker for LDAP
- Configure Docker to run silent mode

Network Security Groups

RDS Gateway Server:	HTTPS Inbound restricted to Alan Turing Institute IP range
Lunix Based Servers:	ALL traffic to Internet blocked except for Azure services (Backup, OMS etc)
RDS Session Hosts:	ALL traffic to Internet blocked except for Azure services (Backup, OMS etc)

Operation Management Suite

A new OMS (Log analytics) subscription is created

- OMS workspace = DOMAINNAME
- Resouce Group = <RESOURCE GROUP>
- Region = UK South
- Pricing = OMS per node

- Create automation account in OMS Resource group
  - Name: <AUTOMATION ACCOUNT>
- All VMs within the environment are connected
- The following solutions are added:
  - AD Assessment
  - Agent Health
  - Alert Management
  - Antimalware Assessment
  - Activity Logs Analytics
  - Change Tracking
  - DNS Analytics
  - Security and Audit

Azure Extension Installation

- All the VMs have the following extensions installed (before NSG implemented)
  - IaaS Antimalware
  - OMS agent

- Run Agent update on Git Lab Server
  - Install upgrade:
    - sudo apt-get install walinuxagent
  - Restart agent
    - sudo initctl restart walinuxagent

Azure Recovery Services

- Azure Recovery Services enabled
- All VMs added to the vault
- Backup Enabled to allow the server to backup disk encrypted VMs
- Standard backup policy
    - Daily backup @ 11PM
    - 15 day retention

Azure Disk Encryption

Azure Disk encryption is enabled on all Windows based VMs and Git Lab Servers. Data Science and Hack MD server cannot be disk encrypted within Azure.