

Red Forest RDS Build Guide (Please read thoroughly and follow every step)

RDS Prerequisites:

1. 8 VMs
2. All machines will require WinRM configured (Check the technical section in a later section of this document)
3. Microsoft NPS Extension for MFA already installed and configured with Azure (link provided at the end of this document). See Document NPSExtensionDeploy for instructions
4. File share for mounting profile disks. To calculate for maximum needed is size of profile disk (default is 20gb) x number of users
5. Certificate. RDS requires 2 certificates 1 Web/Gateway and 1 Broker. It's easier to use 1 certificate instead of having to create and manage 2. See Document Guide to creating certificate for RDS
6. Msonline module on the NPS Server
7. All VMs should be fully patched. Due to some security exploits some domain security policies may block rdp from working.
8. In server manager for All RDS Servers add all rds machines into under the systems management. (This is mandatory or rds deployment will fail)
9. Both broker servers should have Microsoft ODBC DRIVER 17 for sql server. Download the bigger of the 2 files which is the 64bit version. Link here:
<https://www.microsoft.com/en-us/download/details.aspx?id=56567>
10. Follow SQL Server build guide for SQL Configuration

Technical Prerequisites:

The powershell script will build the following farm

2x Web/Gateways

2x brokers

2x session host

1x sql server

1x nps mfa server

WinRM:

Run the following command on all machines:

Enable-psremoting -force -skipnetworkprofilecheck

To view WinRM configs you can run:

WinRM Enumerate Winrm/Config/Listener

or

WinRm Get WinRM/Config

To Test and Verify Functionality:

Test-Wsman -computename (remote computer)

Add if needed: -authentication Basic/Default/Negotiate/Kerberos/Digest/Credssp

And/Or: -credential (get-credential)

RDS Autobuild script

The rdsdeploywithha.ps1 will build you our default build of

2x web/gateway servers

2x session hosts

2x broker

1x nps

1x sql server

Set your license server to per user

Open an administrative powershell

&"path to script\RDSDeploy.ps1"

User Input:

1. Fill out all the information under "variables"
2. You will be prompted to enter the rds the Secret Key.
3. You must do search and replace on for the following items
#search and replace "\$Domain\group" with actual domain\group no quotes
#RDS Build Orchestrator for High Availability Build
#install rsat tools if it's not already installed
#search and replace "\$Domain\group" with actual domain\group no quotes

#search and replace "\$groupsid1" with actual groupsid_output from below for group sid
command no quotes
###Get RDS GroupNameSID copy output SID and paste this below
#\$rdsgroupname="RDS group name only NO domain"
#\$sid=(get-adgroup -identity \$rdsgroupname).sid
#\$groupsid=\$sid|select-object value
#\$groupsid #<-----Grab this output for \$groupsid1

#search and replace "\$nps1" with nps_fqdn no quotes
#search and replace "\$sharedsecret1" with sharedsecret no quotes
#search and replace "\$Web1a" with fqdn of web1 no quotes
#search and replace "\$Web2a" with fqdn of web2 no quotes
#search and replace "\$gate1" with fqdn of web1 no quotes
#search and replace "\$gate2" with fqdn of web2 no quotes
#search and replace "\$rdsusergroup1" with rds user group in domain\usergroup format
no quotes
#search and replace "\$gatewayfqdn1" with fqdn of front end of rds gateway like
"rd.domain.com" no quotes
#search and replace "\$clientaccessname1" with fqdn of rds broker client accessname
like "rds.domain.com" no quotes

#search and replace "\$web1ip", \$web2ip, \$brkr1ip, \$brkr2ip and fill in the respective IPs

Instructions:

1. Follow document "Guide for Creating Certificate for RDS"
2. Follow document "Guide to Setting Up Azure MFA Extension for NPS"
3. Follow document "Guide to SQL Server Build for RDS"
4. RDS is deployed on/from a remote host (because of reboots). Best done from a management host. Copy the script rdsdeploywithha.ps1 here.
5. Makes sure you fill out all the variables and finish the search and replace items.
6. This build script is fully automated if all instructions are followed and the servernames are set correctly.

Resources:

Azure NPS Extension for MFA

<https://www.microsoft.com/en-us/download/details.aspx?id=54688>