node 'windows.example.com' {

file {['c:/NTDS']:

ensure => directory

}

dsc\_windowsfeature {'dns':

dsc\_ensure => 'Present',

dsc\_name => 'DNS',

}

dsc\_windowsfeature { 'addsinstall':

dsc\_ensure => 'Present',

dsc\_name => 'AD-Domain-Services',

}

dsc\_windowsfeature {'addstools':

dsc\_ensure => 'Present',

dsc\_name => 'RSAT-ADDS',

}

dsc\_windowsfeature {'addnstools':

dsc\_ensure => 'Present',

dsc\_name => 'RSAT-DNS-Server',

}

dsc\_xwaitforaddomain {'DscForestWait':

dsc\_domainname => 'ad.contoso.com',

dsc\_domainusercredential=> {

'user' => 'Administrator@ad.contoso.com',

'password' => Sensitive(lookup('password'))

},

dsc\_retrycount => 55,

dsc\_retryintervalsec => 10,

subscribe => Dsc\_windowsfeature['addsinstall'],

}

dsc\_xaddomaincontroller {'ReplicaDC':

dsc\_domainname => 'ad.contoso.com',

dsc\_domainadministratorcredential => {

'user' => 'Administrator@ad.contoso.com',

'password' => Sensitive(lookup('password'))

},

dsc\_safemodeadministratorpassword => {

'user' => 'admin',

'password' => 'Passw0rd01'

},

dsc\_databasepath => 'C:\NTDS',

dsc\_logpath => 'C:\NTDS',

dsc\_sysvolpath => 'C:\SYSVOL',

subscribe => Dsc\_xwaitforaddomain['DscForestWait'],

}

#this applies to AWS/Azure machines only

exec { 'Check if DNS is set automatically':

command => 'Set-DnsClientServerAddress -InterfaceAlias "Ethernet" -ResetServerAddresses',

unless => 'if (!((netsh interface ipv4 show dns | select-string "DNS servers configured through DHCP:") -match "DNS servers configured through DHCP:")) {exit 1}',

provider => powershell,

logoutput => true,

}

reboot {'dsc\_reboot':

subscribe => Dsc\_xaddomaincontroller['ReplicaDC'],

message => 'DSC has requested a reboot',

}

}