

getWindows: Active Directory (AD) Server

Authors: Cameron Sullivan (RIP), Kody Moseley, Joe Patton, Llewellyn Searing, Nick Dieff

New DC setup	1
Backup DC Setup	2
AD Administration from Powershell	2
Tasks	3
Special Task: Join a Client to an AD Domain	3
Special Task: Change Domain Name	4

New DC setup

Uses Powershell to create a clean domain controller in a fresh environment.

Pre-requisites:

- Make sure the computer name of the DC is correct (hostname).
 - Have a static IP address.
1. Install the “AD-Domain-Services” feature
 - a. > Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
 2. Import the Powershell module
 - a. > Import-Module ADDSDeployment
 3. Install-ADDSForest -DomainName <my domain>
 - a. Note that the Powershell AD commands will be installed at this time as well.
 - b. You may also want the -InstallDNS option to create a DNS server

The default users will be:

- Administrator
- Guest
- Krbtgt
- Possible service accounts (sshd...)

There will be a great number of default groups (~48), under the CNs “Users” and “Builtin”. AD default group descriptions: <http://bit.ly/2mKnoD1>.

Backup DC Setup

If you already have a working AD forest with at least one domain controller, you can easily create some secondary controllers that can be used in case of failures.

The local admin password, safemode password, and AD Admin password MUST all be different. When creating a credential, be sure to include the domain name in the username: <domain name>\<user name>.

1. Install the "AD-Domain-Services" features
 - a. > Install-WindowsFeature AD-Domain-Services -IncludeManagementTools
2. Import the Powershell module
 - a. > Import-Module ADDSDeployment
3. Create a Powershell Credential with the administrator password for your domain
 - a. \$cred = New-Object -TypeName System.Management.Automation.PSCredential -ArgumentList "<domain name>\Administrator", (read-host -asSecureString "Admin Password")
4. Promote the current computer to a domain controller inside of your domain
 - a. Install-ADDSDomainController -Credential \$cred -DomainName "<domain name>"
 - b. -InstallDNS is also available as an option here. The DNS records will be replicated between servers if the zone is AD connected

AD Administration from Powershell

Powershell ad module reference: <https://bit.ly/2NWtH3X>

To use these Powershell commands, you will need to have RSAT installed:

```
> Get-WindowsCapability -Name Rsat.ActiveDirectory* -Online |
Add-WindowsCapability -Online
```

On Server 2008 / Win7 you will need to run the command after: Import-module ActiveDirectory

Filtering

Many of the commands from the ActiveDirectory module have a -Filter subcommand. This takes as an argument a string in "Powershell Expression Language". Here are some examples:

```
> Get-ADUser -Filter * # returns all users
> Get-ADUser -Filter {GivenName -like "Chris"} #Users with the first name chris
> Get-ADUser -Filter {Name -like "Patenaude*"} # get all of Joe's relatives
# note that the name parameter stores the name in the form <Last>, <first>
```

Find AD users

```
> Get-ADUser -Filter *
```

To get extra properties like “sn”, “LastLogonDate”, or “whenChanged”, add them as arguments to the -Properties option, or use *-Properties * to view all. Note that not all properties appear for every user.

Here’s a few useful searches:

```
> Get-AdUser -filter { PasswordNeverExpires -eq $true -and Enabled -eq $true }
```

Add new users

```
> New-ADUser -Name "<name>" -SamAccountName "<username>" -AccountPassword  
(Read-Host -AsSecureString) -Enabled $True -GivenName "<first name>" -Surname "<last  
name>" -Path "CN=Users,DC=<domain>,DC=<tlid>" -UserPrincipalName  
"<username>@<domain>"
```

Add users to groups

First, find the name of a group you want. Then:

```
> Add-ADGroupMember "<group name>" -Members <member1, member2...>
```

Check group members

```
> Get-ADGroupMember -Identity <group name>
```

Optionally add the -Recursive argument to also show members of subgroups.

Kick them out of a group

```
> Remove-ADGroupMember -Identity DocumentReaders -Members DavidChew
```

Reset a user’s password

```
> Set-ADAccountPassword <user> -Reset -NewPassword (ConvertTo-SecureString  
-AsPlainText '<new password>' -Force)
```

Set a user’s password expiration

```
> Set-ADUser <user> -PasswordNeverExpires $true
```

Add a new computer object

```
> Add-ADComputer
```

Enable User

```
> Enable-ADUser -Identity <user>
```

Tasks

Active Directory quick-reference from Microsoft: <http://bit.ly/2m2aIPQ>

Special Task: Join a Client to an AD Domain

With Gui

- Ensure that the client is using the AD DC as its DNS server.
- Navigate: computer > System properties > Advanced system settings > Computer Name
- At the bottom under the “Member of” tab, select Dom Getain and add the domain name.

- Click "OK," and enter the credentials of a domain admin.

With Powershell


> Add-Computer -DomainName "<YourDomainName>" -Credential (Get-Credential)

You can use Remove-Computer to de-join a machine as well.

Special Task: Change Domain Name

NOTE: Before completing domain name change, record old DNS name and NetBIOS name.

- Use `random /list` command to create the XML file (located in current directory of command prompt).
- Open the newly created XML file which shows the current domain name, indicated in the `DNSname` and `NetBiosName` fields.



```

<NetBiosName></NetBiosName>
<DcName></DcName>
</Domain>
<Domain>
  <!-- PartitionType:Application -->
  <Guid>1e12b9b7-8617-4e2f-b7b3-7bbbadcdf270</Guid>
  <DNSname>ForestDnsZones.milksuckers.com</DNSname>
  <NetBiosName></NetBiosName>
  <DcName></DcName>
</Domain>
<Domain>
  <!-- ForestRoot -->
  <Guid>44fea925-280c-4066-b6a2-ec4a26d3967e</Guid>
  <DNSname>milksuckers.com</DNSname>
  <NetBiosName>MILKSUCKERS</NetBiosName>
  <DcName></DcName>
</Domain>
</Forest>

```

Edit the XML file with the domain name changes.

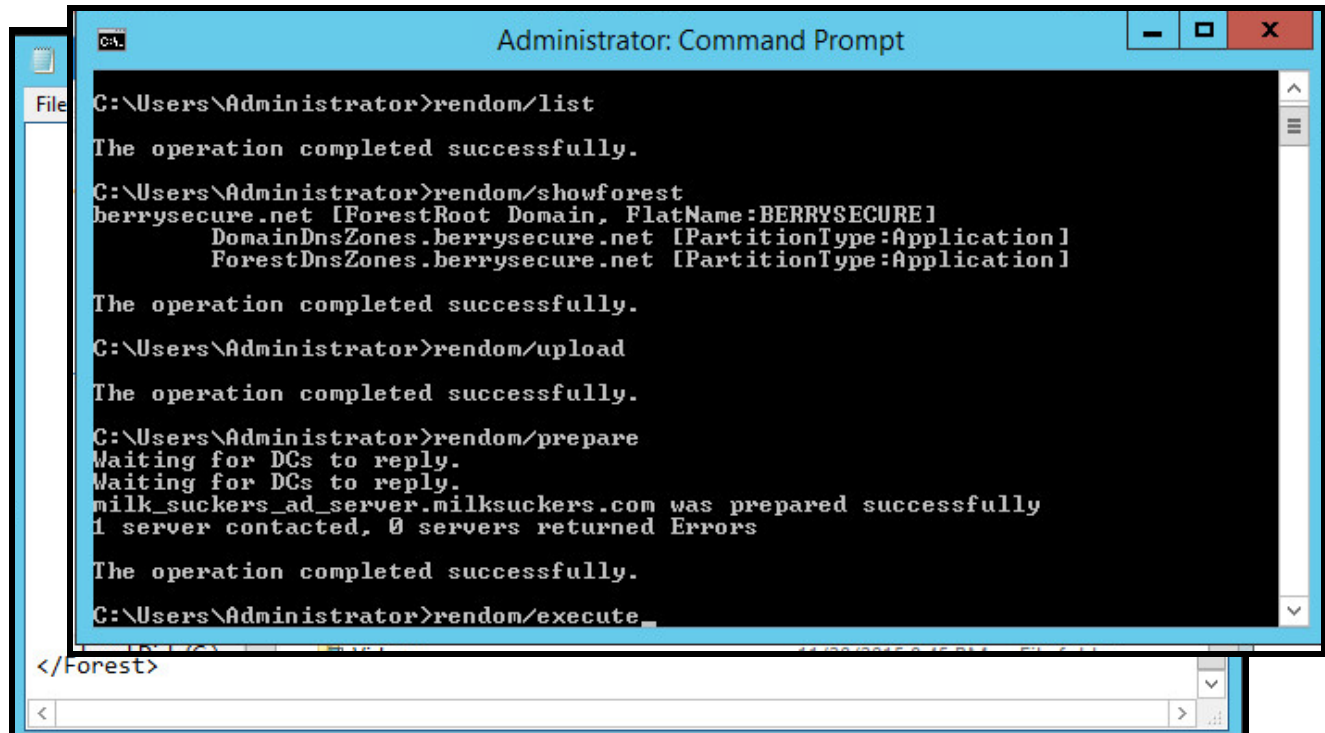


```

<?xml version="1.0"?>
<Forest>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>456e9ed1-29bc-4b51-944f-582d5fb2b9b8</Guid>
    <DNSname>DomainDnsZones.berrysecure.net</DNSname>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- PartitionType:Application -->
    <Guid>1e12b9b7-8617-4e2f-b7b3-7bbbadcdf270</Guid>
    <DNSname>ForestDnsZones.berrysecure.net</DNSname>
    <NetBiosName></NetBiosName>
    <DcName></DcName>
  </Domain>
  <Domain>
    <!-- ForestRoot -->

```

To ensure that the domain name change was proceeding as expected, give the `rendom /showforest` command. Then, use the `rendom /upload` command. Next, to prepare to the change, execute the `rendom /prepare` command.



```

Administrator: Command Prompt

C:\Users\Administrator>rendom/list
The operation completed successfully.

C:\Users\Administrator>rendom/showforest
berrysecure.net [ForestRoot Domain, FlatName:BERRYSECURE]
  DomainDnsZones.berrysecure.net [PartitionType:Application]
  ForestDnsZones.berrysecure.net [PartitionType:Application]
The operation completed successfully.

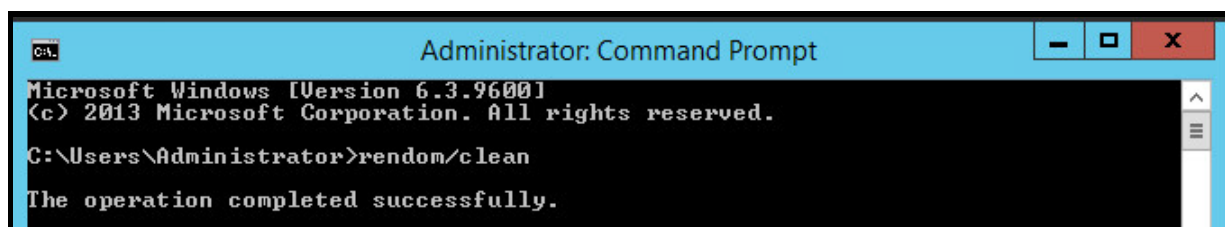
C:\Users\Administrator>rendom/upload
The operation completed successfully.

C:\Users\Administrator>rendom/prepare
Waiting for DCs to reply.
Waiting for DCs to reply.
milk_suckers_ad_server.milksuckers.com was prepared successfully
1 server contacted, 0 servers returned Errors
The operation completed successfully.

C:\Users\Administrator>rendom/execute_

```

After using the command `rendom /execute`, complete the domain rename process by using the `rendom /clean` command.



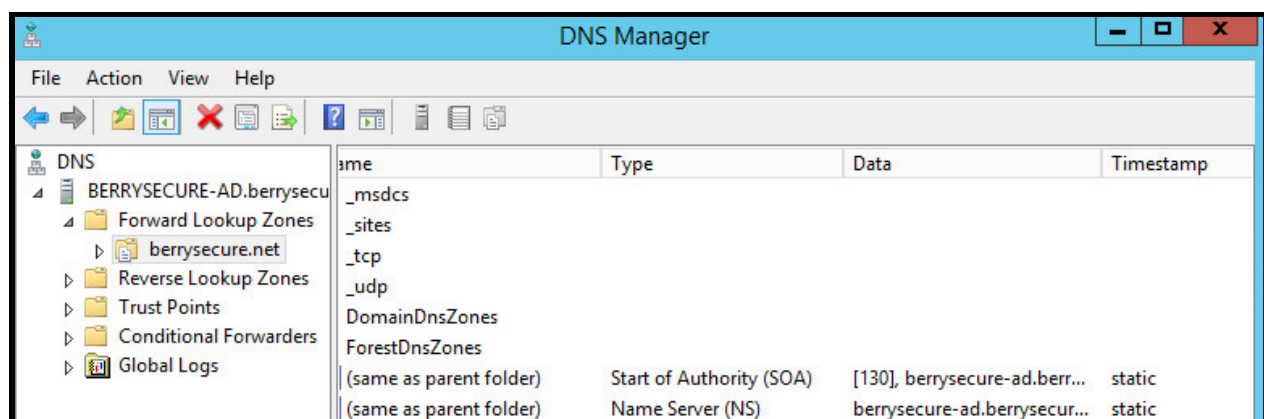
```

Administrator: Command Prompt

Microsoft Windows [Version 6.3.9600]
(c) 2013 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>rendom/clean
The operation completed successfully.

```



```
C:\Users\Administrator>nslookup www.berrysecure.net  
1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.ip6.arpa  
primary name server = 1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.  
0.0.0.0.0.0.0.0.ip6.arpa  
responsible mail addr = <root>  
serial      = 0  
refresh     = 28800 <8 hours>  
retry       = 7200  <2 hours>  
expire      = 604800 <7 days>  
default TTL = 86400 <1 day>  
  
Server:    UnKnown  
Address:    ::1  
  
Name:       www.berrysecure.net  
Address:    10.50.1.20
```

NOTE: After completing the change, the gpfixup command must be used to resolve the domain name change for other applications. First navigate to C:\ directory, then use the following syntax:

```
gpfixup /olddns:OLD_DNS_NAME /newdns:NEW_DNS_NAME /oldnb:OLD_NETBIOS_NAME /dc:NEW_DNS_NAME 2>&1 >gpfixup.log
```

```
> Get-ADGroupMember -Identity "Global Admins"
```

```
> Add-ADUser -Name "Marina"
```

```
> Add-ADGroupMember -Identity "Global Admins" -Members "Marina"
```