invis-sub-setup - action #46718

Create a setup-script for invis-sub-server

2019-01-26 15:49 - flacco

Status:	In Progress	**Start date:**	2019-01-26
Priority:	Normal	**Due date:**	
Assignee:		**% Done:**	30%
Category:		**Estimated time:**	0.00 hour
Target version:	1.0		

Description

Major steps to realize with this Script:

1. Establish an openVPN connection to the main invis-server
2. Join the Domain as a "Read Only Domain Controller" (RODC)
3. Setup sssd
4. Setup local samba shares
5. realize (owncloud based) data synchronization between sub and main-server

Some of these steps are already realized inside the joininvis-script from the invisAD-client package.

Joining the domain as a rodc (https://de.wikipedia.org/wiki/Read_Only_Domain_Controller) instead of a simple member server seems to be the better way. In a productive environment at one of our custumers I tried to realize a subsidiary server as a simple member-server. Nearly every time the vpn-connection caused by a not very stable internet-connection, I had to rejoin the domain with the sub-server to give the sub-users access to their local samba-shares.

Related issues:

Related to invis-sub-setup - action #38303: Create a rpm package with basic d...	**In Progress**	**2018-07-07**

History

#1 - 2019-01-26 15:52 - flacco

Infos about using samba as a rdoc: https://wiki.samba.org/index.php/Join_a_domain_as_a_RODC

#2 - 2019-01-26 16:19 - flacco

As in invisAD-setup, this script here has to switch from networkmanager to wicked.

#3 - 2019-01-26 16:34 - flacco

- Status changed from Feedback to In Progress

- % Done changed from 0 to 10

The setup-Script is based on sine2 and called subsine

#4 - 2019-01-27 08:08 - flacco

- Related to action #38303: Create a rpm package with basic directories, config files and dependencies added

#5 - 2019-01-27 08:13 - flacco

subsine module "check" works for now.

Next step is module "quest". The module has to ask for the following informations:

1. Internet-FQDN from the master invis-server
2. Path to the vpn client certificate (p12 file) (?)
3. Password for p12 file
4. AD-Domain
5. Internet-FQDN from the sub-server
6. DNS Forwarders

From the invisAD-setup we keep the following questions:

1. admin contact
2. clean transfer (only needed, if we realize a transfer-share)

3. SMTP SASL informations
4. monitoring system

We also keep the randomized creation of SSH and HTTPs Ports

#6 - 2019-01-27 08:45 - flacco

subsine modules and running order - first draft:

1. check
2. quest
3. sysprep
4. vpn (establish a vpn connection during setup. If this fails subsine has to break)
5. samba (join domain as a rodc)
6. dns (from sine2 with ad backend)
7. mailserver (postfix should be able to send mails via the organisations smarthost)
8. fileserver
9. firewall (from sine2 - reduced)
10. monitoring (from sine2)

#7 - 2019-01-27 09:08 - flacco

Questions about VPN-connection:

Should we realize a bridged Network-2-Network (N2N) connection or fits a simple routed Client-2-Network (C2N) our needs?

I added a openvpn configuration file as a first draft for a C2N connection to the package.

The file contains two placeholders:

Attribute: "remote" - Placeholder: remote-fqdn
Attribute: "pkcs12" - Placeholder: invis-server.p12

The file contains the askpass-directive, means that we have to place a passwordfile for the p12-file in /etc/openvpn/keys.

#8 - 2019-11-17 16:33 - flacco

- % Done changed from 10 to 30

There are some "subsine" modules ready:

1. check
2. quest
3. sysprep
4. nameserver
5. openvpn

#9 - 2019-11-27 18:30 - flacco

The first productive test shows, that acting as a router an dhcp-server seems to be a good idea. In my first testcase, the internet provider is unitymedia and it is a business contract with one static ip-address. In this case the router (FritzBox) acts only as default gateway, no dhcp-server. In this case the the invis-sub-server needs two NICs and the external one is statically configured to the static ip-address from unitymedia.

This meens, we should use the network-setup from invis-Server also for the invis-sub-server.

#10 - 2019-11-27 18:32 - flacco

the dhcp-server setup should be simple, with a ascii-based configuration.

First step is to realize just a simple address-pool for the sub-servers subnet.

#11 - 2020-05-30 22:43 - flacco

- Target version set to 1.0

#12 - 2021-09-17 04:42 - flacco

Next steps to go:

1. dhcp-Server module
2. fileserver module
3. firewall module