GSD. Network - Info Pool - Network related information

Article ID: KB0039826
Created: 2024-12-19 14:03:39
Updated: 2024-12-19 14:03:39
Author: {'link': 'https://fmcnadev.service-now.com/api/now/table/sys_user/acaf843397d74958f7e3bb8fe153afe3', 'value': 'acaf843397d74958f7e3bb8fe153afe3'}
Category: {'link': 'https://fmcnadev.service-now.com/api/now/table/kb_category/b513d404c3ca1a100acd3300150131fb', 'value': 'b513d404c3ca1a100acd3300150131fb'}

General Information:

Possible symptoms/errors:

User wants to know more network related info.

Alternative names of the system:

N/A

IMPORTANT NOTICE:

N/A

Solution:

This article lists network related changes and particularities.

[Table of contents will follow]

Location's infrastructural information

Go to "https://one.intra.fresenius.com/display/FNCHOT/Locations+and+details" to see the information about the network infrastructure for several locations.

smb1protocol (SMB1)

Please be advised to not activate the "smb1protocol" on user's computer anymore!

In detail it's: "Enable-WindowsOptionalFeature-Online-FeatureName smb1protocol" which can be run via Windows Powershell.

After this command the computer needs to be reinstalled. Furthermore, the SMB1 protocol has been deactivated on the servers!

Blocked RDP

As being announced on the 11th of March 2021:

"We would like to inform you that recent vulnerabilities of MS products and possible exploits are leading us to the need of implementing some immediate measures. For all Fresenius Digital Technology clients, we already actively deactivated RDP on these clients via GPO. For all Netcare managed servers we are blocking all external RDP connections by our Firewalls and only granting 10.0.0.0/8 (FGN) to have RDP access to the servers via GPO.

Expected business impact is quite limited because the firewalls are already blocking the traffic, but we want to be on the save side and therefore also block the traffic via GPO.

In case of any impact on client site, please contact digitalworkplace-hardware-packaging@fresenius.com.”

Inter- and Intranet

Request for internet access

All users who want to access the internet, need to request access by filling out the according request form for "Secure Web Access" in the ServiceShop: Secure Web Access Exception (I000843)

Check access rights and group memberships

To see if a user has internet access rights, there are three locations to check:

The field "employeeType" in the according user's person document's details in Lotus Notes must be set to "STD". If it is empty, it needs to be filled. If it says "AZB" it means "Auszubildender" ("Apprentice") which stands for restricted access (e.g., no Facebook) .There you can also check whether a HTTP password is set or net by having a look at "HTTPPassword". An encrypted password should be shown.Check the user account's group memberships in AD. The user needs to be a member of "GG-DE-EK1-InternetAccess"Check the ZSCaler proxy. The needs needs there be a member of “GG-DE-EK1-InternetAccess” group and not of "Default" only

VPN

Today a significant amount of users (around 4000) still use the old VPN gateway without MFA which brings technical and security based issues. As a result, access to vpn-access.fresenius.com and vpn-gw.fresenius.com will be disabled on the 22nd of April 2022.

Therefore, the CA01 and EJBCA certificates are removed from Fresenius managed devices for all users that:

have an Azure AD account,have activated MFA or have a license and can do it.

As a result, old gateways should not be accessible for them. The VPN team won’t physically decommission gateways until further notice. They are also going to change the ASA profile on vpn-access@fresenius.com. Currently this gateway accepts only CA09 certificates, and the team will remove CA09 and ad CA01. Since this is non-MFA VPN, they can’t allow to access it with CA09 certificate.

Certificate Validation Error

A "Certificate Validation Error" means that the certificate of the VPN gateways is not accepted by the client as being valid. This can happen if:

the root certificate hasn't been installed in the client (is distributed via MS group policies or something comparable onto all managed clients)the time is not correct (Windows system time)

A CRL check of the certificate should actually not take place explicitly. If it's activated on the client it might cause this problem. Experience shows that with a new certificate the behavior changes.

If the issue occurs again, please check the following:

open https://vpn-gw.fresenius.de via web browsercheck in the browser if the certificate is shown as "valid" (click on the lock icon in front of the URL)if the Root-CA of FNC-CA1 is missing it can be imported into the browser via http://ek1-cms02.hg.fresenius.de:8080/ejbca/retrieve/ca_certs.jsp

Check own certificate

Users can check their own certificate as follows:

In Windows click on STARTEnter: certmgr.msc and press ENTERSelect "Own certificates", expand it via double click and select "Certificates"

NAC (Network Access Control)

NAC is implemented in several locations in Bad Homburg. The latest implementation was in RP3 and MB1 in December of 2020 and in D15, S15 and S21 in January of 2021.

D16, DO1, EK2 and Horexstrasse 28-32 were changed in the end of January 2021.

Possible tickets that indicate a problem on this topic (e.g.: no network access), please forward to the ServiceNow group: “Int_WW_Office-Infrastructure_DIaaS_SLS_FNC”.

Please categorize potential tickets like this:

Service Offering : Network Services LANCategory: FailureSubcategory: Connectivity

Contacts:

https://fnc.service-now.com/nav_to.do?uri=%2Fkb_view.do%3Fsysparm_article%3DKB0014355%26sysparm_stack%3D%26sysparm_view%3D

Assignment Group:

N/A

Ticket Creation:

Template: N/ACategorization:

Configuration Item: N/ACategory: N/ASubcategory: N/A

Important Links:

Contacts and groups

https://fnc.service-now.com/nav_to.do?uri=%2Fkb_view.do%3Fsysparm_article%3DKB0014355%26sysparm_stack%3D%26sysparm_view%3D

http://ek1-cms02.hg.fresenius.de:8080/ejbca/retrieve/ca_certs.jsphttps://vpn-gw.fresenius.de