NNPTC Network Startup

Last Updated By: Wes Wilson
Last Updated: 2/22/2025

NOTE 1: Preferentially use the Administrators credentials for all logins. If necessary, breakglass credentials can be retrieved from Thycotic Secret Server (while it is available) or the breakglass password book. Breakglass credentials will be denoted with an alphanumeric code in superscript that can be matched to the credential in Secret Server (or book) for ease of reference

NOTE 2: The Links page should be utilized for easy navigation to required management portals and resources: `Z:\Shared\NNPTC\W_Drives\ISD\Links\Links-VDI.html`

General Flow and Steps

1. Restore Support Equipment and UPSs

1. Ensure power is on at the CRAC Units
2. [CRAC1] Log in to the console for each CRAC unit. Turn the unit ON.
3. Go to each COM closet. Plug in the UPS and ensure it is *Online* and supplying power.
4. Plug in the UPSs in P120 and D107, verify they are *Online*.
5. Verify the UPS in P201A is online and supplying power via the *inverter*
    1. <Procedure to bring UPS online>

2. Networking Infrastructure

1. Turn on the *Core* switches (NNPP - **NNPTC-D216-01** and NNTP - ~~**PTCLW-SW-01**~~)
2. Turn on the [NNTP] Firewalls (**Palo Alto Firewall 01**, **Palo Alto Firewall 02**)

Make sure the core switches are fully online before continuing (~10 minutes) The lights on the active ports will be green when it is up.

3. KVMs

Turn on the KVMs (NNPP and NNTP)

4. Restore Services

4.a - Domain Controllers

Power on the Domain Controllers:

- **NNPTC1DC21**
- **NNPTC1DC22**
- **PTCW16P-DC06**
- **PTCW16P-DC07**
- **PTCLW22P-DC01** (NNTP)

** Wait for these servers to come online fully before proceeding.** Verify using the KVM or other means.

4.b - Authentication Servers (Cisco Identity Services Engine (ISE))

1. Turn on all of the *primary* ISE Nodes

    - **NNPTC-D216-ISE-03** (NNPP)
    - **PTCL-ISE-03** (NNTP)

    Wait at least 5 minutes. It will take ~15 minutes for the application server to fully come online.

    To monitor services, [ISE1] log in to the ISE server via KVM or SSH Client (SecureCRT or PuTTY). Enter the following command: `show application status ise`

2. Power on secondary ISE nodes

    - **NNPTC-D216-ISE-04** (NNPP)
    - **PTCL-ISE-04** (NNTP)

4.c - DHCP

Using the [KVM1] KVM or [IDRAC1] iDRAC, power on the *primary* DHCP servers

- **NNPTC1BU03** (NNPP)
- **PTCLW16P-BU01** (NNTP)

4.d - Cluster Nodes and Other Services

1. Power on the following servers:

    - Primary SQL Cluster Node (**NNPTC1SQ18**)
    - Primary File Cluster Node (**NNPTC1FS10**)
    - SCCM Relay Server (**PTCLW19P-SCCM04**)
    - Hyper-V Management Server (**NNPTC1VM04**)

    Wait for these servers to come online fully before proceeding

2. [TR1] Log in to the Hyper-V Management Server (**NNPTC1VM04**). Open Hyper-V Manager and power on the Trellix servers in the following order:

    1. Trellix Database Server (**NNPTC1EPOSQL03**). Wait for services to come online.
    2. Trellix Management Server (**NNPTC1EPO03**)

3. [SA1] Log in to the *primary* File Cluster Node (**NNPTC1FS10**)

4. Power on the secondary Cluster Nodes

    - Secondary File Cluster Node (**NNPTC1FS11**)
    - Secondary SQL Cluster Node (**NNPTC1SQ17**)

5. (**Optional**) Clean up DNS entries for Virtual Desktops:

    1. Open DNS Management
    2. (NNPP) Remove all entries matching NNPTC-VM* from the NNPTC1.nnpp.gov DNS Zone
    3. (NNTP) Remove any entries matching PTCLW1[0,1]V*

4.e - Nutanix

1. Turn on each host in each of the Nutanix Appliances

Block 6	Block 7	Block 8
NNPTC-NTNX-06-01	NNPTC-NTNX-07-01	NNPTC-NTNX-08-01
NNPTC-NTNX-06-02	NNPTC-NTNX-07-02	NNPTC-NTNX-08-02
NNPTC-NTNX-06-03	NNPTC-NTNX-07-03	NNPTC-NTNX-08-03
NNPTC-NTNX-06-04	NNPTC-NTNX-07-04	NNPTC-NTNX-08-04

4.f - Badgescanners

1. Verify each Badgescanner blade pc is fully seated in the chassis.
2. Power them on.
3. UltraVNC may be used to monitor the badgescanner sessions remotely.
4. The HTA Dashboard (IPRT Status page) may be used to see the last badgescanner state and determine the blade/PAD configuration.

Potential troubleshooting tips for the I/PORTS can be found at the end of this documentation.

5. Starting the VDI

1. Using the Links page (see above), log in to each ESXi Host using the appropriate vSphere Web Client

ESX1 Block 6 vSAN	ESX1 Block 8 vSAN	ESX1 NNTP vSAN
NNPTC1ESX0601	NNPTC1ESX0801	PTCLVM-ESX0201
NNPTC1ESX0602	NNPTC1ESX0802	PTCLVM-ESX0202
NNPTC1ESX0603	NNPTC1ESX0803	PTCLVM-ESX0203
NNPTC1ESX0604	NNPTC1ESX0804	PTCLVM-ESX0204
		PTCLVM-ESX02M

2. In the vSphere window for each ESXi Host, click the *Inventory* link and expand the server list
3. Take the ESXi host out of *Maintenance Mode*
    1. In the vSphere web client, click the **Actions** button and select **Exit Maintenance Mode**
4. Start the Nutanix Controller VMs (CVMs)
    1. On each host, right click on the Nutanix Controller VM (**NTNX-*-CVM**) and select **Open Console**
    2. If the CVM is not running, select **VM -> Power -> Power On** from the menu
    3. Click inside each console and press enter
    4. Press the key-combination `CTRL + ALT` to release the cursor from the console window

    NOTE: The CVMs are fully online when each is at a login prompt
5. Using an SSH Client (SecureCRT or PuTTY), [NT1] log in to one of the Nutanix CVMs (on each cluster) to restore the cluster storage

Example CVMs for each Cluster	
Block 6	nnptc-ntnx-06-01.nnptc1.nnpp.gov
Block 7	nnptc-ntnx-07-01.nnptc1.nnpp.gov
Block 8	nnptc-ntnx-05-01.nnptc1.nnpp.gov

    1. Enter the username and password
    2. Enter the command `cluster start` in the console
    3. Verify the cluster has started by issuing the command `cluster status`

       All CVMs should report having a process ID (PID) for each service listed

6. Locate the ESXi host with the vCenter appliance installed.

vCenter Servers	
Block 6	NNPTC1VC0601
Block 8	NNPTC1VC0801
NNTP	PTCL-VC0101

    1. Click the *Virtual Machines* link
    2. Right click on the server console. Select **Open Browser Console**.
    3. On the Action Menu, select **Power -> Power On**

7. Log into each vCenter server ([VC2] **NNPTC1VC0601**, [VC1] **NNPTC1VC0801**, [VC1] **PTCL-VC0101**)

    1. Select the *VMs and Templates* view
    2. Start and VMs that are not started, **ignore any VMs beginning with 'x'**.
        1. Right click on each VM and select **Power -> Power On**

8. From the cVenter interface for the Cluster, for each ESXi host:

    1. Click the **Summary** tab
    2. Click the **Edit** button in the **Custom Attributes** window
    3. Change the value of `InstantClone.Maintenance` from `2` to `0`
    4. Select the **vCenter** at the top of the system tree
        1. Click on the **Configure** tabb
        2. Click **Advanced Settings**
        3. Click the **Edit** button
        4. Select the *filter* icon and type `vcls`
        5. Set the Value to `True`
        6. Click **Save**
        7. Click **Save** again

6. Start up Nutanix AHV

1. Using an SSH Client (SecureCRT or PuTTY) [NT1] log in to each AHV host

    1. Issue the following command - `virsh list -all | grep CVM`
    Note the name of the CVM and whether it is running. If it is not running, execute the next command
    2. `virsh start CVM_NAME` where 'CVM_NAME' is returned from the above command

2. [NT1] Using an SSH Client (SecureCRT or PuTTY), log in to <IP Address>.

    1. Issue the command `cluster start`

    2. Verify the cluster has started by issuing the command `cluster status | more`

        All CVMs should report having a process ID (PID) for each service listed.

3. Using the Links page (see above), [NT1] log in to Prism Element

    1. Click on **Home** and selec **VM**

    2. Click on **Table**

    3. Click on each VM in the list and then click the *Power* link (located above the graphs)

        Elasticstack Servers (**NNPTC1ELAS0X**) should be powered on in **ASCENDING** order

4. Using the Links page (see above), log in to the applicable VMWare Horizon View console ([SA1] **Block 8 Horizon**, [SA1] **Block 6 Horizon**, [SA2] **NNTP Horizon**)

    1. Enable all desktop pools and provisioning for each pool

        1. Select ALL pools
        2. Select *Enable Desktop Pool*
        3. Click 'OK' when prompted
        4. Select ALL pools
        5. Select *Enable Provisioning*
        6. Click 'OK' when prompted

        NOTE: If any errors occured during the above actions, attempt the enablement on an individual pool (vice all pools).

7. Restore CommVault

1. Turn on the CommVault Nodes (**NNPTC1CV01**, **NNPTC1CV02**, **NNPTC1CV03**)

2. Once booted, use an SSH Client (SecureCRT or PuTTY) to [CV1] log in to each node

3. Execute `df -h` on each node. This enumerates the mounted volumes on the node.

    Ensure the `/ws/glus` volume is mounted

4. If the services on the nodes do not start within 30 minutes as noted in the `commvault list` command, run the command `commvault -all restart`

5. From CommCell, remove any blackout window that may be in effect.

8. Verification Steps

Badgescanner Troubleshooting