Integrating the Tactical Datacenter extended storage

12/19/2019 • 7 minutes to read •

In this article

Integration prerequisites

Preparation and health check steps

Automated configuration steps

Post-automation validation steps

Security hardening steps

Shut down

Next steps

This article provides guidance for integrating the extended storage hardware in the Tactical Datacenter in a supported and updated state. The last steps in this document are to validate that the shares are communicating with the integrated Azure Stack system.

Integration prerequisites

- Azure Stack Partner Toolkit version 1.1912.x.x or later, used to deploy and generate deployment files.
- Azure Stack deployed and healthy.
- Isilon hardware deployed per the hardware integration guide and healthy with no errors. Call support to address any errors before proceeding.
- The Azure Stack **DeplomentData.json** file used for Azure Stack deployment. This file can be found on the HLH in D:\AzureStack.

  The configuration script pulls the following information from this file:
  - The Azure Stack internal fully qualified domain name (FQDN).
  - Information about the ‘Extended Storage Management’ subnet: gateway address and Isilon chassis IP address range (lower and upper).
  - Information about the ‘Extended Storage’ subnet (used for data access): Isilon node address range (lower and upper), SmartConnect service address, gateway

address, and subnet size.

- Isilon ‘root’ account password.
- Avocent password for the serial connection.
- Credentials for the CloudAdmin account from the Azure Stack domain.
- IP address and credentials for the HLH OS.
- Connection to OneFS via the management subnet. This connection can be done on node 1 of each chassis on interfaces: 1,5,9,13,17,21,25,29,33. For example, OneFS and CLI management can take place from 100.73.1.4
- OneFS version 8.2.1.0.

Preparation and health check steps

1. Make sure the Isilon system is started up. For instructions, see the Start up section of Administering the extended storage of Tactical Datacenter.
2. Make sure the system is healthy and the hardware has no amber lights.
3. Make sure all network connections on the switches and the Isilon system are healthy, including the back-end and front-end network.
4. Log in to Avocent and check for any errors by running the following command from the console:

   console Copy

   ```
   isi status
   ```

   Contact Microsoft support to get help on issues with using the extended storage for Tactical Datacenter.
5. Log in to the HLH OS.
   a. Connect to the management node 1 IP address in the system zone to pull up the OneFS web UI in your browser. For example, go to https://100.73.1.4:8080 and enter the credentials to log in.
6. In OneFS, make sure the system is healthy.
   a. Clusters should show green.

b. Check Cluster Management, Events, and Alerts. Resolve any issues that are no longer relevant.

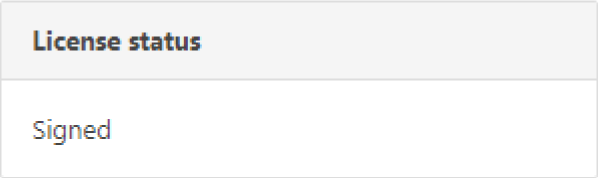
c. Check dashboard to verify the health of the nodes, drives, and cluster.

d. Contact Microsoft support to get help on issues with using the extended storage for Tactical Datacenter.

7. Make sure Cluster Management and licensing is in place.

   a. In the OneFS web UI, go to: **Cluster management** -> **Licensing**.

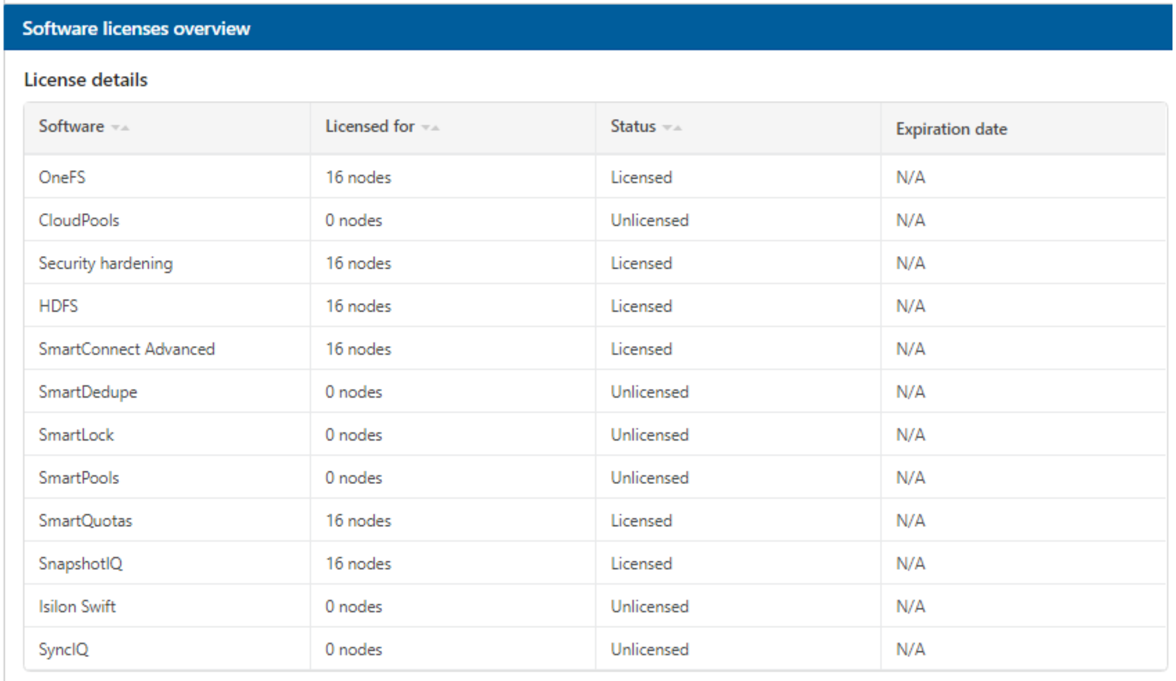
   b. Make sure the status is signed:



License status

Signed

   c. Make sure all licenses below are in place:



Software licenses overview

License details

Software	Licensed for	Status	Expiration date
OneFS	16 nodes	Licensed	N/A
CloudPools	0 nodes	Unlicensed	N/A
Security hardening	16 nodes	Licensed	N/A
HDFS	16 nodes	Licensed	N/A
SmartConnect Advanced	16 nodes	Licensed	N/A
SmartDedupe	0 nodes	Unlicensed	N/A
SmartLock	0 nodes	Unlicensed	N/A
SmartPools	0 nodes	Unlicensed	N/A
SmartQuotas	16 nodes	Licensed	N/A
SnapshotIQ	16 nodes	Licensed	N/A
Isilon Swift	0 nodes	Unlicensed	N/A
SyncIQ	0 nodes	Unlicensed	N/A

8. In the OneFS web UI, go to: **Cluster management** -> **General settings**.

   Make sure the date, time, and information on the Cluster Identity tab is set correctly.

Automated configuration steps

This section outlines the necessary steps to run the automated configuration of the Isilon environment and to integrate with the Azure Stack environment.

1. Log in to the HLH as administrator.

2. Start Powershell.exe in administrator mode and run the following commands:

   a. PowerShell Copy

   ```
   cd C:\OEMSoftware\ExtendedStorage
   ```

   b. PowerShell Copy

   ```
   $rootcred = Get-Credential -Credential 'root'
   ```

   This credential is used by the script to make changes to the Isilon system. When prompted, enter the password for the 'root' account.

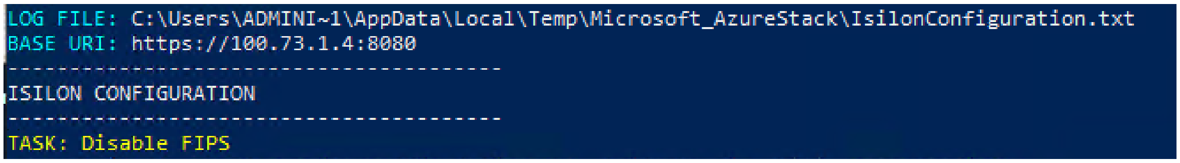
   c. PowerShell Copy

   ```
   .\Invoke-ExtendedStorageConfiguration.ps1 -IsilonConfig -RootCred
   $rootcred
   ```

   This command starts the automated configuration script. It will read the configuration settings from the DeploymentData.json and configure the Isilon system as required by Azure Stack.

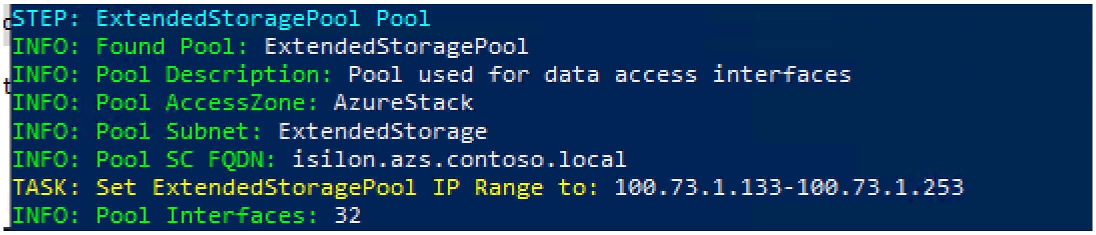
   Note

   You may see a message "TASK: Disable FIPS" and the script will exit. If this happens, create the `$rootcred` object again (step b) and re-run the script (step c).



```
LOG FILE: C:\Users\ADMINI~1\AppData\Local\Temp\Microsoft_AzureStack\IsilonConfiguration.txt
BASE URI: https://100.73.1.4:8080
----------------------------------------
ISILON CONFIGURATION
----------------------------------------
TASK: Disable FIPS
```

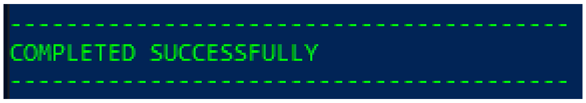
Once the script is running, settings that are found to already be set correctly will be displayed with a green "INFO:" heading. Items that are being set by the script will be displayed with a yellow "TASK:" heading as shown below:



```
STEP: ExtendedStoragePool Pool
INFO: Found Pool: ExtendedStoragePool
INFO: Pool Description: Pool used for data access interfaces
INFO: Pool AccessZone: AzureStack
INFO: Pool Subnet: ExtendedStorage
INFO: Pool SC FQDN: isilon.azs.contoso.local
TASK: Set ExtendedStoragePool IP Range to: 100.73.1.133-100.73.1.253
INFO: Pool Interfaces: 32
```

You can rerun this script multiple times if needed to ensure that all required items are shown with the green “INFO:” label. This label indicates that all settings are correct.

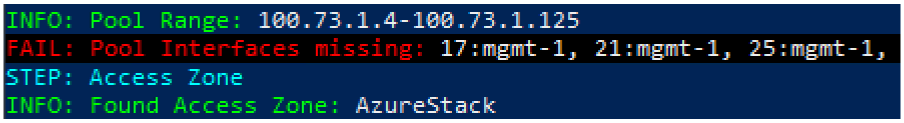
At successful completion of the script, the following message will be displayed:



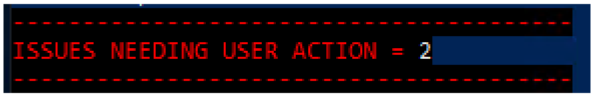
```
---------------------------------------
COMPLETED SUCCESSFULLY
---------------------------------------
```

Items that couldn't be set correctly will be displayed with a red “FAIL:” message and you'll see a message at the end of the script indicating that manual intervention may be required to resolve these issues. You can run the same command again to see if the failure was due to an intermittent issue.

[Contact Microsoft support](#) to get help on issues with using the extended storage for Tactical Datacenter.



```
INFO: Pool Range: 100.73.1.4-100.73.1.125
FAIL: Pool Interfaces missing: 17:mgmt-1, 21:mgmt-1, 25:mgmt-1,
STEP: Access Zone
INFO: Found Access Zone: AzureStack
```



```
---------------------------------------
ISSUES NEEDING USER ACTION = 2
---------------------------------------
```

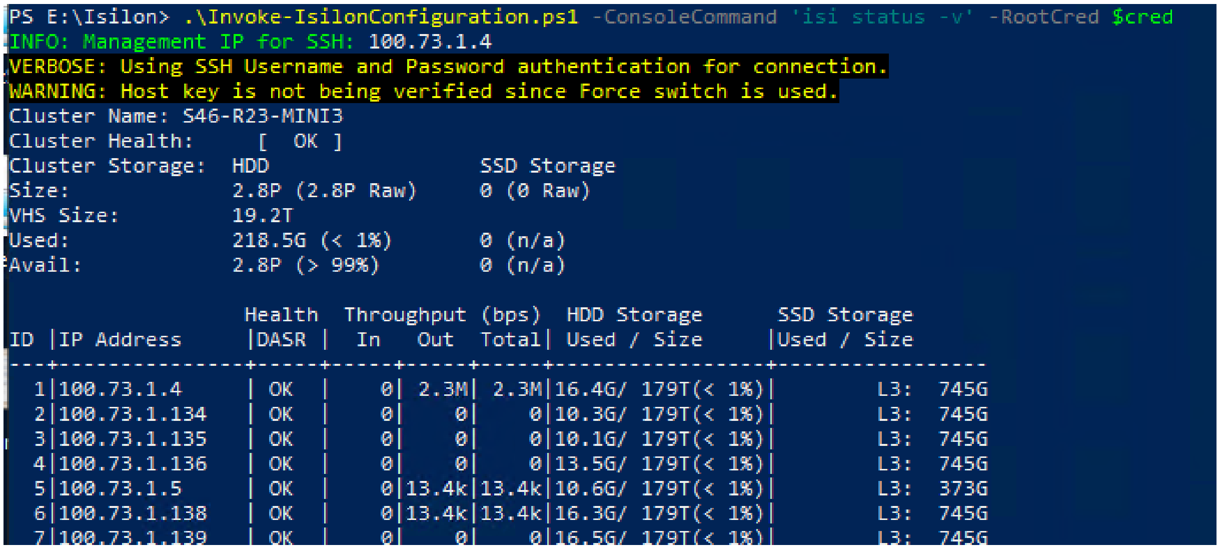
d. Keep this PowerShell session open as it will be used for the next steps.

> **Tip**
>
> The `Invoke-ExtendedStorageConfiguration.ps1` script can be used to execute OneFS CLI commands via SSH.

Example:

PowerShell Copy

```powershell
.\Invoke-ExtendedStorageConfiguration.ps1 -ConsoleCommand 'isi status -v'
-RootCred $rootcred
```



```
PS E:\Isilon> .\Invoke-IsilonConfiguration.ps1 -ConsoleCommand 'isi status -v' -RootCred $cred
INFO: Management IP for SSH: 100.73.1.4
VERBOSE: Using SSH Username and Password authentication for connection.
WARNING: Host key is not being verified since Force switch is used.
Cluster Name: S46-R23-MINI3
Cluster Health:     [  OK ]
Cluster Storage:  HDD                 SSD Storage
Size:             2.8P (2.8P Raw)     0 (0 Raw)
VHS Size:         19.2T
Used:             218.5G (< 1%)       0 (n/a)
Avail:            2.8P (> 99%)        0 (n/a)

                   Health  Throughput (bps)  HDD Storage      SSD Storage
ID |IP Address      |DASR |  In   Out  Total| Used / Size     |Used / Size
---+----------------+-----+-----+-----+-----+-----------------+----------------
  1|100.73.1.4      | OK  |    0| 2.3M| 2.3M|16.4G/ 179T(< 1%)|        L3:  745G
  2|100.73.1.134    | OK  |    0|    0|    0|10.3G/ 179T(< 1%)|        L3:  745G
  3|100.73.1.135    | OK  |    0|    0|    0|10.1G/ 179T(< 1%)|        L3:  745G
  4|100.73.1.136    | OK  |    0|    0|    0|13.5G/ 179T(< 1%)|        L3:  745G
  5|100.73.1.5      | OK  |    0|13.4k|13.4k|10.6G/ 179T(< 1%)|        L3:  373G
  6|100.73.1.138    | OK  |    0|13.4k|13.4k|16.3G/ 179T(< 1%)|        L3:  745G
  7|100.73.1.139    | OK  |    0|    0|    0|16.5G/ 179T(< 1%)|        L3:  745G
```

3. The next step is to integrate Isilon with the Azure Stack domain.

> ⓘ **Note**
>
> This only works on Azure Stack builds 1.1912.0.20 (and higher) as the modules scripts used by this automation are built into Azure Stack.

The script below performs the following actions:

- Adds static routes on the Azure Stack domain controllers for the Isilon Management network.
- Joins the Isilon cluster to the Azure Stack domain.
- Configures user access and access control lists (ACLs) on the Isilon share.
- Azure Stack configuration of the Isilon share.

a. If you're not in the correct directory, run:

PowerShell | Copy

```powershell
cd C:\OEMSoftware\ExtendedStorage
```

b. Run the following command but replace `DOMAIN` with the Azure Stack domain name and provide the password for the `cloudadmin` user.

PowerShell | Copy

```powershell
$azsCred = Get-Credential -Credential 'DOMAIN\cloudadmin'
```

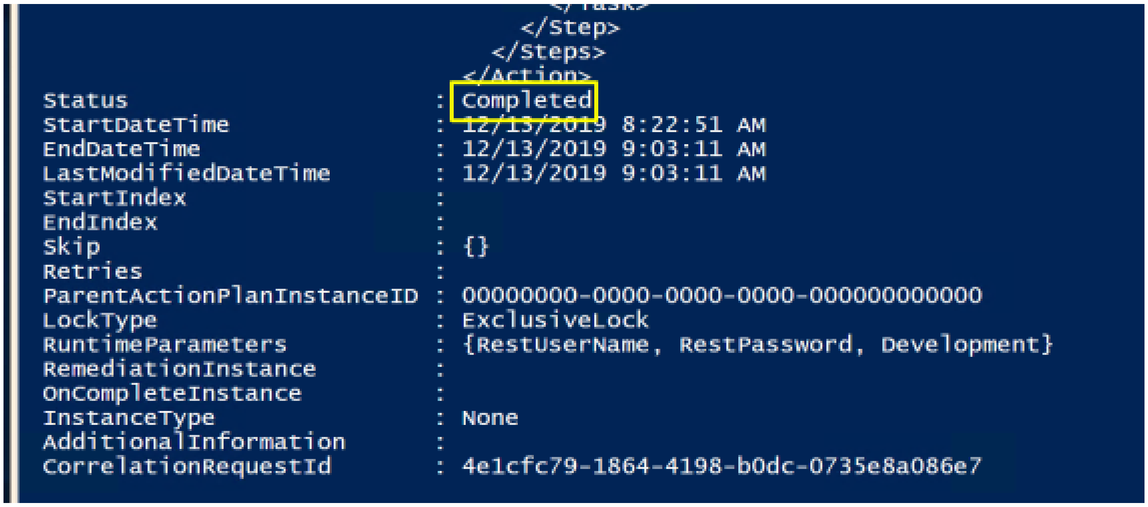
c. Create an object containing the parameters required for Add-NasCluster by running the following command:

PowerShell Copy

```powershell
.\Invoke-ExtendedStorageConfiguration.ps1 -AddNasCluster -RootCred
$rootcred -AzureStackCred $azsCred`
```

d. Wait until all actions finish with status showing 'Completed'. **This process could take 30 minutes or more**.

When it's done, the status will show as completed:



```
                                </Task>
                              </Step>
                            </Steps>
                          </Action>
Status                      : Completed
StartDateTime               : 12/13/2019 8:22:51 AM
EndDateTime                 : 12/13/2019 9:03:11 AM
LastModifiedDateTime        : 12/13/2019 9:03:11 AM
StartIndex                  :
EndIndex                    :
Skip                        : {}
Retries                     :
ParentActionPlanInstanceID  : 00000000-0000-0000-0000-000000000000
LockType                    : ExclusiveLock
RuntimeParameters           : {RestUserName, RestPassword, Development}
RemediationInstance         :
OnCompleteInstance          :
InstanceType                : None
AdditionalInformation       :
CorrelationRequestId        : 4e1cfc79-1864-4198-b0dc-0735e8a086e7
```

ⓘ Note

If the Add-NasCluster command couldn't be found, try to import the module first by running: `Import-Module Microsoft.Azurestack.NasCluster.psm1`.

Post-automation validation steps

1. Reboot the Cluster:
   a. In the OneFS web UI, go to: **Cluster management** -> **Hardware configuration**.
   b. Select the **Cluster** tab.
   c. Select **Reboot cluster**.
   d. Wait 5-10 minutes, then log back in to the OneFS portal and clear related events that occurred during the cluster reboot.

2. Contact Microsoft support to get help on issues with using the extended storage for Tactical Datacenter.

Security hardening steps

Now that the configuration and validation steps are completed, the system is ready to harden its security with Defense Information Systems Agency (DISA) Security Technical Implementation Guides (STIGs). This system won't use SmartLock or WORM, it will use STIGs and other hardening settings detailed in the steps below.

To meet federal Approved Products List (APL) requirements, the configuration of OneFS must comply with STIGs that define hardening configuration requirements. STIGs are maintained by DISA, which produces STIGs for several computing technologies, referred to as assessment areas. STIG hardening is designed for Isilon clusters that support federal government accounts. Clusters that don't support federal government accounts are generally not candidates for STIG hardening.

> ⓘ **Note**
>
> STIG hardening assumes that the entire environment has been hardened to STIG standards.

An extended storage solution is only one piece of a complex installation and coexists with the surrounding physical and electronic environment. You must develop and maintain comprehensive security policies for the entire environment. It's assumed that you've implemented the following security controls before Isilon security deployment:

- Physical security of computer room facilities.
- Comprehensive network security.
- Monitoring of computer-related controls, including:
  - Access to data and programs.
  - Secure organizational structure to manage login and access rights.
  - Change control to prevent unauthorized modifications to programs.
  - Service continuity to ensure that critical services and processes remain operational if there's a disaster or data breach.

The security hardening steps are:

1. Run:

PowerShell Copy

```
$rootcred = Get-Credential -Credential 'root'
```

This credential is used by the script to make changes to the Isilon system. When prompted, enter the password for the ‘root’ account.

2. From an elevated PowerShell session, run:

   PowerShell Copy

   ```
   .\Invoke-ExtendedStorageConfiguration.ps1 -SecurityHardening -RootCred
   $rootcred
   ```

3. Run health checks against both Azure Stack and the extended storage. For information on how to check for health, see Checking health for the Tactical Datacenter extended storage.

4. From an active SSH connection to a management interface (for example, 100.73.1.4), run:

   PowerShell Copy

   ```
   isi hardening apply --profile=STIG
   ```

   > **Note**
   >
   > The STIG profile apply process will take 30-60 minutes to complete.

5. Run health checks against both Azure Stack and the extended storage. For information on how to check for health, see Checking health for the Tactical Datacenter extended storage.

Shut down

Shut down system for shipping. For instructions, see Shutting down the Tactical Datacenter extended storage.

Next steps

[Configure and set up the extended storage for the Tactical Datacenter solution]

Is this page helpful?

👍 Yes 👎 No