PowerScale OneFS

Security Configuration Guide

9.1.0.0

October 2020

DELL EMC

Network security

OneFS security includes the security of networked subsystems and interfaces.

Network exposure

The following sections detail the network exposure of OneFS, including ports, protocols, services exposed, and default states.

Network port usage

Standardized protocols enable other system units to exchange data with OneFS.

The TCP/IP protocol suite uses numbered ports to describe the communication channel within the protocol. Generally, the OneFS system uses a well-known port for receiving incoming data. The client uses that ephemeral port number to send data. Port numbers and IP addresses are included with a data packet, which enables other systems to make determinations about the data stream. TCP and UDP protocols within the TCP/IP suite use ports that range from 1 to 65535.

The Internet Assigned Numbers Authority (IANA) assigns and maintains port numbers. They are divided into three ranges:

1. Well-known ports, ranging from 0 to 1023.
2. Registered ports, ranging from 1024 to 49151.
3. Dynamic or private ports, ranging from 49152 to 65535.

Protocols support both IPv4 and IPv6 addresses except where noted.

NOTE: As a security best practice, use an external firewall to limit access to the cluster to only those trusted clients and servers that require access. Allow restricted access only to ports that are required for communication. Block access to all other ports.

Port	Service name	Protocol	Connection type	Usage and description	Effect if closed	Default on installation
20	ftp-data	TCP	Outbound	• FTP access (disabled by default) • Data channel for FTP service	FTP access is unavailable.	Disabled
21	ftp	TCP	Inbound	• FTP access • Control channel for FTP access	FTP access is unavailable.	Disabled
22	ssh	TCP	Inbound	• SSH login service • console management **NOTE:** does not support IPv6.	SSH secure shell access is unavailable.	Enabled
25	smtp	TCP	Outbound	Email deliveries	Outbound email alerts from OneFS are unavailable.	Disabled
53	DNS	UDP	Outbound	Domain Name Service resolution	Services not able to resolve domain names.	Enabled
53	DNS	TCP/UDP	Inbound	SmartConnect DNS requests and incoming DNS request responses	SmartConnect DNS resolution is unavailable.	Enabled
80	http	TCP	Inbound	HTTP for file access	HTTP access to files is unavailable.	Disabled
88	kerberos	TCP/UDP	Outbound	Kerberos authentication services that are used to authenticate users against Microsoft Active Directory domains	Kerberos authentication is unavailable.	Disabled

SSH security best practices

This section provides recommendations for restricting SSH access and disabling root SSH access to the cluster. You can perform one or more of these procedures, depending on what is best for your environment.

Restrict SSH access to specific users and groups

By default, only the SecurityAdmin, SystemAdmin, and AuditAdmin roles have SSH access privileges. You can grant SSH access for specific cluster management tasks to users and groups that have more restricted roles.

To perform these steps, you must log in as a user who has the ISI_PRIV_ROLE privilege, which allows you to create roles and assign privileges.

1. Open a secure shell (SSH) connection to any node in the cluster and log in.
2. Create a custom role by running the following command, where *<role_name>* is the name of the custom role:

```
isi auth roles create <role_name>
```

3. Add the ISI_PRIV_LOGIN_SSH privilege to the role:

```
isi auth roles modify <role_name> --add-priv ISI_PRIV_LOGIN_SSH
```

4. Add a user or a group to the role by running one or both of the following commands, where *<user_name>* is the name of the user, and *<group_name>* is the name of the group:

```
isi auth roles modify <role_name> --add-user <user_name>
```

```
isi auth roles modify <role_name> --add-group <group_name>
```

Disable root SSH access to the cluster

Disabling root SSH access to the cluster prevents attackers from accessing the cluster by brute-force hacking of the root password.

After disabling root SSH access, you can still log in as root by performing one of the following actions:

- Physically connect to the cluster using a serial cable, and log in as root.
- Open a secure shell (SSH) connection to any node in the cluster and log in using an RBAC-authorized account. At the command prompt, type **`login root`** and press ENTER. Type the root password when prompted. This method has the security benefit of requiring two passwords (the user password and the root password).

You can also elevate the privileges for select users to give them access to specified root-level commands (see the *Privilege elevation: Assign select root-level privileges to non-root users* section of this guide).

1. Ensure that there is at least one non-root administrator account that is configured and working, and that allows remote SSH login to the cluster, before you disable root SSH access.
2. Open a secure shell (SSH) connection to any node in the cluster and log in as root.
3. Disable root access by running the following command:

```
isi ssh modify --permit-root-login=false
```

Disable forwarding of Unix domain and TCP sockets

Disabling forwarding of Unix domain and TCP sockets prevents attackers from TCP and stream forwarding vulnerabilities.

1. Open a secure shell (SSH) connection to any node in the cluster and log in as root.

2. Run the following commands:

```
isi_gconfig -t ssh-config allow_tcp_forwarding=no
isi_gconfig -t ssh-config allow_stream_local_forwarding=no
```

Data-access protocols best practices

To prevent unauthorized client access through unused or unmonitored protocols, disable protocols that you do not support. For those protocols that you do support, limit access to only those clients that require it.

The following sections provide instructions for limiting or disabling these protocols.

Use a trusted network to protect files and authentication credentials that are sent in cleartext

The security between a client and the PowerScale cluster depends which protocol is being used. Some protocols send files and/or authentication credentials in cleartext. Unless you implement a compensating control, the best way to protect your data and authentication information from interception is to ensure that the path between clients and the cluster is on a trusted network. Even if you do implement a compensating control, a trusted network provides an additional layer of security.

Use compensating controls to protect authentication credentials that are sent in cleartext

Some protocols send authentication credentials in cleartext. You can use compensating controls to enable more secure authentication.

Protocols that send authentication credentials in cleartext include:

- FTP
- HDFS (and WebHDFS)
- HTTP
- NFS
- Swift

Compensating controls for cleartext authentication in OneFS include:

- Kerberos authentication (supported by some protocols).
- NTLM authentication (supported by some protocols).
- Secure impersonation on HDFS.
- Enabling TLS on the FTP service.
- SSH tunneling (wraps an existing non-secure protocol and moves all communication to an encrypted channel).
- The OneFS API (all authentication credentials are sent over TLS).

Use compensating controls to protect files that are sent in cleartext

Files specific to the web interface are sent over TLS. Files specific to `/ifs` are sent differently depending on the protocol. You can use compensating controls to increase the security of files that are sent in cleartext.

Protocols that may send `/ifs` data files in cleartext include:

- FTP
- HDFS (and WebHDFS)
- HTTP
- NFS
- Some versions of SMB

6. Open the `/ifs/data/backup/webui_httpd.conf` and the `/etc/mcp/templates/apache24.conf` files in a text editor.
7. Add the following lines to the very bottom of the file (after `</VirtualHost>`):

```
# Begin Security Best Practices
Header always append X-Frame-Options SAMEORIGIN
Header always append X-Content-Type-Options nosniff
Header always append X-XSS-Protection "1; mode=block"
# End Security Best Practices
```

8. Confirm that the changes are correct. Then save the file and exit the text editor.
9. Copy the updated file to the `/etc/mcp/templates` directory on all nodes in the cluster:

```
isi_for_array 'cp /ifs/data/backup/webui_httpd.conf \
/etc/mcp/templates/webui_httpd.conf'
```

```
isi_for_array 'cp /ifs/data/backup/apache24.conf \
/etc/mcp/templates/apache24.conf'
```

10. (Optional) Delete the working and backup copies from the `/ifs/data/backup` directory:

```
rm /ifs/data/backup/webui_httpd.conf \
/ifs/data/backup/webui_httpd.conf.bak
```

```
rm /ifs/data/backup/apache24.conf \
/ifs/data/backup/apache24.conf.bak
```

Accept up-to-date versions of TLS in the OneFS web interface

If required, configure the OneFS web administration interface to accept transmissions from the most up-to-date versions of the TLS protocol.

If your current configuration at `/etc/mcp/templates/webui_httpd.conf` contains `+TLSv1` or `+TLSv1.1`, install the latest security patches. For more information, see the Current PowerScale OneFS Patches document on the Customer support site.

6

Glossary

Topics:

- Terminology

Terminology

The following terms and abbreviations describe some of the features and technology of the PowerScale OneFS system and PowerScale cluster.

Access-based enumeration (ABE)	In a Microsoft Windows environment, ABE filters the list of available files and folders to allow users to see only those that they have permissions to access on a file server.
Access control entry (ACE)	An element of an access control list (ACL) that defines access rights to an object (like a file or directory) for a user or group.
Access control list (ACL)	A list of access control entries (ACEs) that provide information about the users and groups allowed access to an object.
ACL policy	The policy that defines which access control methods (NFS permissions and/or Windows ACLs) are enforced when a user accesses a file on the system in an environment that is configured to provide multiprotocol access to file systems. The ACL policy is set through the web administration interface.
Authentication	The process for verifying the identity of a user trying to access a resource or object, such as a file or a directory.
Certificate Authority (CA)	A trusted third party that digitally signs public key certificates.
Certificate Authority Certificate	A digitally signed association between an identity (a Certificate Authority) and a public key to be used by the host to verify digital signatures on public key certificates.
Command-line interface (CLI)	An interface for entering commands through a shell window to perform cluster administration tasks.
Digital certificate	An electronic ID issued by a certificate authority that establishes user credentials. It contains the user identity (a hostname), a serial number, expiration dates, a copy of the public key of the certificate holder (used for encrypting messages and digital signatures), and a digital signature from the certificate-issuing authority so that recipients can verify that the certificate is valid.
Directory server	A server that stores and organizes information about a computer network's users and network resources, and that allows network administrators to manage user access to the resources. X.500 is the best-known open directory service. Proprietary directory services include Microsoft Active Directory.
Group Identifier (GID)	Numeric value used to represent a group account in a UNIX system.
Hypertext Transfer Protocol (HTTP)	The communications protocol used to connect to servers on the World Wide Web.
Hypertext Transfer Protocol Secure (HTTPS)	HTTP over TLS. All network traffic between the client and server system is encrypted. In addition, HTTPS provides the option to verify server and client identities. Typically, server identities are verified and client identities are not.
Kerberos	An authentication, data integrity, and data-privacy encryption mechanism that is used to encode authentication information. Kerberos coexists with NTLM and provides authentication for client/server applications using secret-key cryptography.

Lightweight Directory Access Protocol (LDAP)	An information-access protocol that runs directly over TCP/IP. LDAP is the primary access protocol for Active Directory and LDAP-based directory servers. LDAP Version 3 is defined by a set of Proposed Standard documents in Internet Engineering Task Force (IETF) RFC 2251.
LDAP-based directory	A directory server that provides access through LDAP. Examples of LDAP-based directory servers include OpenLDAP and SUN Directory Server.
Network File System (NFS)	A distributed file system that provides transparent access to remote file systems. NFS allows all network systems to share a single copy of a directory.
Network Information Service (NIS)	A service that provides authentication and identity uniformity across local area networks and allows you to integrate the cluster with your NIS infrastructure. Designed by Sun Microsystems, NIS can be used to authenticate users and groups when they access the cluster.
OneFS API	A RESTful HTTP-based interface that enables cluster configuration, management, and monitoring functionality, and enables operations on files and directories.
OpenLDAP	The open source implementation of an LDAP-based directory service.
Public Key Infrastructure (PKI)	A means of managing private keys and associated public key certificates for use in Public Key Cryptography.
Secure Sockets Layer (SSL)	A security protocol that provides encryption and authentication. SSL encrypts data and provides message and server authentication. SSL also supports client authentication if required by the server.
Security Identifier (SID)	A unique, fixed identifier used to represent a user account, user group, or other secure identity component in a Windows system.
Server Message Block (SMB)	A network protocol used by Windows-based computers that allows systems within the same network to share files.
Simple Network Management Protocol (SNMP)	A protocol that can be used to communicate management information between the network management stations and the agents in the network elements.
Support Remote Services Gateway	Secure Remote Support (SRS) enables 24x7 proactive, secure, high-speed remote monitoring and repair for many Dell EMC products.
Transport Layer Security (TLS)	The successor protocol to SSL for general communication authentication and encryption over TCP/IP networks.
User Identifier (UID)	Alphanumeric value used to represent a user account in a UNIX system.
X.509	A widely used standard for defining digital certificates.