OpenText Open Enterprise Server 23.4

Release Notes

April 2024

Legal Notices

Contents

About This Release Notes 5

1 What’s New or Changed in OES 23.4 7

1.1 What’s New or Changed in OES 23.4 Updated ISO 7
1.2 What’s New or Changed in OES 23.4 7
1.2.1 Rebranding 8
1.2.2 OES Welcome Page. 8
1.2.3 Channel Upgrade 8
1.2.4 Unified Management Console 8
1.2.5 Distributed File Services (DFS) 9
1.2.6 Common Internet File System (CIFS) 10
1.2.7 . . . . Centralized Certificate Management. 10
1.2.8 Cloud Integrated Storage (CIS). 10
1.2.9 iPrint 11
1.2.10 Domain Services for Windows (DSfW) 11
1.2.11 NetWare Core Protocol (NCP) 11
1.2.12 Client for Open Enterprise Server 12
1.2.13 . . . . Storage Services File System (NSS) 12
1.2.14 DNS / DHCP 13
1.2.15 Unchanged Components in OES 23.4 13
1.3 OES Entitlements 13

2 Service Issues 15

2.1 OES Installation, Upgrade and Update. 15
2.1.1 Package Conflict Issue 15
2.1.2 Channel Upgrade Issue. 16
2.1.3 Upgrade Issue in SUSE Xen Hypervisor Environment 16
2.1.4 NCS and Upgrade Issue 17
2.1.5 OES Server Registration to MFSMT Fails. 17
2.2 Client for Open Enterprise Server. 17
2.2.1 On Enabling NCP Encryption Disable Send File Support 17
2.2.2 Accessing OES File Copy Utility in Windows Explorer Issue 17
2.2.3 OES File Copy Utility Notifies Incorrect File Size 17
2.2.4 OES File Copy Utility Fails for DFS Junction Volume. 18
2.3 Distributed File Services (DFS) 18
2.3.1 Windows Cannot Access Error. 18
2.3.2 CIFS eDir User can Access Non-OES Windows Target DFS Junction 18
2.3.3 Non-OES Target Validation Errors 19
2.3.4 NCP Clients Issues. 19
2.3.5 iManager Issues 19
2.3.6 RME must be Configured for DFS Junction Pointing to Multiple Targets. 19

2.3.7 DFS Junction Pointing to Non-OES Target using Windows Domain Name 20
2.3.8 DFSTOOL Command Errors 20
2.4 Business Continuity Clustering (BCC) 20
2.4.1 BCC Connections Fail on Enabling only TLS v1.3 20
2.4.2 Cannot Add a New Volume on a BCC Migrated NSS Pool 21
2.4.3 Multiple-Tree Configurations Are Not Supported 21
2.5 Cloud Integrated Storage (CIS) 21
2.5.1 CIS configuration Fails if the CIS pattern is Selected During OES installation with BIOS Firmware 21
2.6 DNS/DHCP Services 21
2.6.1 DHCP Pattern Conflict 21
2.7 Domain Services for Windows (DSfW) 22
2.7.1 Cannot Configure UMC on DSfW Server. 22
2.7.2 Cannot Create Samba Shares. 22
2.7.3 CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers. 22
2.7.4 Workaround for DSFW Name-Mapped Tree 22
2.7.5 Mixed Mode Configuration is not Supported 23
2.7.6 DSfW Interoperability Issues 23
2.8 eDirectory 23
2.8.1 eDirectory Features Not Supported in OES 23
2.8.2 eDirectory Not Restarting Automatically 24
2.9 Identity Console 24
2.10 iManager 24
2.10.1 Uninstalling Plugins from iManager 3.2.6 Fails 25
2.10.2 Updating and Uninstalling Plugins using iManager Post-OES Upgrade Fails 25
2.10.3 Issues with OES 2023 Cluster Plugin 25
2.11 iPrint Advanced 25
2.11.1 Documents with SmartArt Graphics or Tables 25
2.12 NetWare Core Protocol (NCP). 25
2.12.1 On Enabling NCP Encryption Disable Send File Support 25
2.13 OES Cluster Services (NCS) 25
2.13.1 Cluster Node Crashing Issue 26
2.13.2 Cluster Enabled Linux Volume Creation Failure 26
2.14 OES Remote Manager (NRM) 26
2.14.1 Newly Installed or Upgrade Issue 26
2.14.2 Nagios Service 27
2.14.3 Unable to Perform Group Operations. 27
2.15 OES Storage Services (NSS) 27
2.15.1 RAID 5 Issues 27
2.16 OES User Rights Map (NURM) 27
2.16.1 Unable to Apply Map Rights Using the IDM User Map 27
2.17 Unified Management Console (UMC) 27
2.17.1 UMC Configuration. 27

A Verifying the Integrity of the Downloaded Files 29

B Deprecated Components and Services 31

About This Release Notes

OpenText Open Enterprise Server (OES) 23.4 delivers all the enterprise-class networking, file, and print services that enterprises have relied on for years. OES 23.4 is on SUSE Linux Enterprise 15 SP4, which provides valuable benefits including power savings, virtualization, manageability, and interoperability.

If SUSE removes specific packages from commercial support, those packages are immediately removed from OES channels including supports for them. You can install the removed packages through an external source.

For example, `Midnight Commander` and `icinga2` were automatically removed from the OES channel when SUSE transferred them to Package Hub 15 SP4, which doesn't have any commercial support from SUSE. The only method, which is not supported by us, is to install them from https://download.opensuse.org/repositories/openSUSE:/Backports:/SLE-15-SP4/standard/x86_64/.

NOTE: Micro Focus is now OpenText.

OES 23.4 provides several new features that reduce administrative complexities and provides access to file and storage services regardless of eDirectory or Active Directory as an identity source. For information about the new features, see Chapter 1, "What's New or Changed in OES 23.4," on page 7.

This Release Notes focuses on issues and information that are specific to the OES 23.4 release.

Before installing this release, be sure to review the known issues, as described in "Service Issues" on page 15.

- Chapter 1, "What's New or Changed in OES 23.4," on page 7
- Chapter 2, "Service Issues," on page 15
- Appendix A, "Verifying the Integrity of the Downloaded Files," on page 29
- Appendix B, "Deprecated Components and Services," on page 31

Additional Documentation

For more information about	See
Planning and implementing OES	OES 23.4: Planning and Implementation Guide
Installing, Upgrading, and Updating an OES server	OES 23.4: Installation Guide

Use the following links to access the earlier versions of OES documentation:

- OES 2023 Online Documentation website
- OES 2018 Online Documentation website
- OES 2015 SP1 Online Documentation website

- OES 11 SP3 Online Documentation website
- OES 2 SP3 Online Documentation website
- NetWare 6.5 SP8 Online Documentation website

1 What's New or Changed in OES 23.4

This section summarizes the new features and enhancements in Open Enterprise Server (OES) 23.4 release.

- Section 1.1, "What's New or Changed in OES 23.4 Updated ISO," on page 7
- Section 1.2, "What's New or Changed in OES 23.4," on page 7
- Section 1.3, "OES Entitlements," on page 13

1.1 What's New or Changed in OES 23.4 Updated ISO

You can download the latest OES 23.4 ISO image files from Software Licenses and Downloads (SLD) (https://sld.microfocus.com/mysoftware/index). For more information, see Preparing Physical Media for a New Server Installation in OES 23.4: Installation Guide.

The OES 23.4 Updated ISO includes fixes for the following critical defects:

- **Firewall:** After upgrading from the earlier OES versions to OES 23.4, the firewall is enabled by default.
- **Firewall ports:** After upgrading from the earlier OES version to OES 23.4, the firewall ports are disabled by default.
- **SUSE Xen Hypervisor:** Upgrading from the earlier OES versions to OES 23.4 in a SUSE Xen Hypervisor environment results in eDirectory failure.
- **Splitlock:** The splitlock detect is enabled by default which can result in cluster crash during cluster resource migration or while making clusters online.
- **DSFW Server Error:** Upgrading from the earlier OES versions to OES 23.4 fails, when the eDirectory tree administrator password is not the same as the domain administrator password.

1.2 What's New or Changed in OES 23.4

This section summarizes the new features and enhancements in Open Enterprise Server (OES) 23.4 release.

- Section 1.2.1, "Rebranding," on page 8
- Section 1.2.2, "OES Welcome Page," on page 8
- Section 1.2.3, "Channel Upgrade," on page 8
- Section 1.2.4, "Unified Management Console," on page 8
- Section 1.2.5, "Distributed File Services (DFS)," on page 9
- Section 1.2.6, "Common Internet File System (CIFS)," on page 10
- Section 1.2.7, "Centralized Certificate Management," on page 10
- Section 1.2.8, "Cloud Integrated Storage (CIS)," on page 10

- Section 1.2.9, “iPrint,” on page 11
- Section 1.2.10, “Domain Services for Windows (DSfW),” on page 11
- Section 1.2.11, “NetWare Core Protocol (NCP),” on page 11
- Section 1.2.12, “Client for Open Enterprise Server,” on page 12
- Section 1.2.13, “Storage Services File System (NSS),” on page 12
- Section 1.2.14, “DNS / DHCP,” on page 13
- Section 1.2.15, “Unchanged Components in OES 23.4,” on page 13

1.2.1 Rebranding

Micro Focus is now part of OpenText. Products across the portfolio are now rebranded to reflect OpenText or a more appropriate name. This corporate change impacts the name of products and components, user interfaces, logos, and so on. As a result of this corporate change, OES 2023 SP1 is now referred as OES 23.4.

The documentation is being updated in stages to reflect these changes, including names and screenshots. You can still come across references to Micro Focus in the documentation library until all of the manuals are updated.

1.2.2 OES Welcome Page

The OES Welcome page has been redesigned for an intuitive look and feel and to better manage access to OES resources. In addition, the OES Welcome page is rebranded to reflect the OpenText style. The page highlights the top features for the release along with few important links to Management tools and so on.

After logging in, the user can access to OES resources, community forums, and client downloads from the UMC home page.

1.2.3 Channel Upgrade

Channel upgrade is supported for updating OES 2023 to OES 23.4 using Wagon, Zypper, or Micro Focus Subscription Management Tool (MFSMT).

For more information, see Channel Upgrade from OES 2023 to OES 23.4 or OES 24.3 in OES 23.4: Installation Guide.

1.2.4 Unified Management Console

Managing Open Enterprise Server (OES) services is made easier by the Unified Management Console (UMC). Highly responsive, simple, and secure management tool for managing small and large heterogeneous deployments. As a single point of administration for OES resources, it takes the place of the multiple management consoles.

UMC provides customized access to network administration utilities and content from virtually anywhere using the Internet and a web browser similar to iManager.

Secure Platform

Provides comprehensive security through a token-based authentication system, supported by enhanced authentication methods and Single Sign-On (SSO) enhancements. These measures work in synergy to ensure robust security protocols, safeguarding user access and data integrity while streamlining the authentication process for a seamless user experience.

Highly Responsive UI/UX

Built through strategic utilization of the Angular framework, leveraging its robust capabilities, in tandem with the thoughtful incorporation of UX Aspects, to ensure a highly tailored and user-centric development approach.

Hybrid Management

Utilize effective and efficient management capabilities for maintenance of file and print services, seamlessly supported by the robust eDirectory system. Manage file and print services that have been meticulously integrated with the versatile Active Directory infrastructure.

Simplified Workflows

The platform offers end-to-end workflows, enabling administrators to efficiently manage multiple servers simultaneously. It features a versatile dashboard that provides both basic and advanced analytics, giving users valuable insights into system performance. Additionally, the system incorporates role-based management, allowing for tailored access control and permissions.

New Core Build Ground Up

A centralized REST-based API server, which serves as a lightweight and efficient management service for OES servers. This integrated solution facilitates streamlined server management tasks, promoting efficiency and ease of use for system administrators.

Services Managed in OES 23.4 Release

In this release, you can manage the Server Settings, Storage, Files and Folders, NCP, and Cluster services. For more information, see OES 23.4: Unified Management Console

1.2.5 Distributed File Services (DFS)

Beginning with OES 23.4 release, DFS provides the following enhancements and changes:

- DFS Management Tool (`dfstool`) is a command line utility for managing DFS operations that works only with DFS junctions and Management Context.
- DFS junction now supports non-OES targets along with OES targets.
  - `dfstool` allows you to create the DFS junctions pointing to the target type which can be either OES or non-OES targets.
  - OES supports both NCP and SMB target whereas non-OES supports only SMB targets.
- DFS junction support pointing to multiple OES targets.

For more information, see What’s New or Changed in Distributed File Services in OES 23.4: Distributed File Services Administration Guide for Linux.

1.2.6 Common Internet File System (CIFS)

Large MTU support

To enable and disable support for large MTU, a **novcifs** option has been added. With a large MTU, the maximum data unit size can be up to 1MB, as opposed to 64KB for a normal MTU. A large MTU enables a server to support multi-credit operations and is available from SMB 2.1 or later.

1.2.7 Centralized Certificate Management

Centralized certificate management helps administrators in managing the certificate lifecycle. The features are:

- Mail notifications notify the administrator and the root user of the certificates' impending expiration.
- Indicates where each service's certificates can be found.
- Indicates the certificate's type, such as whether it is self-signed or CA-signed.
- Indicates whether the certificates are still valid.
- Reconfigures the OES services to use a new certificate when certificates are invalid, corrupted or expired.
- A browser-based tool (Unified Management Console, or UMC) that enables remote management of certificates across servers will be available in the upcoming releases.

For more information, see Centralized Certificate Management in OES 23.4: Installation Guide.

1.2.8 Cloud Integrated Storage (CIS)

DST Migration Improvement

To improve the performance and reduce the data migration time from the DST shadow volume to the CIS volume, only folder-level checks are done when multiple migration iterations are performed.

OpenSearch

Beginning with OES 23.4, Elasticsearch is replaced with OpenSearch.

Go, Kafka, and Zookeeper Versions Updated

For improved security, updated to the latest version of Go, Kafka, and Zookeeper.

Infrastructure	Old Version	Updated Version
Go	1.14	1.19
Kafka	Kafka wurstmeister/kafka:2.12-2.5.0	bitnami/kafka:3.4.0
Zookeeper	3.5.7	3.8

1.2.9 iPrint

Secure Communication through IPP

In order to fetch the printer attributes, iPrint has incorporated the feature enhancement of secure communication through IPP on port 443 between the iPrint gateway and printers. To accomplish this feature, the iPrint gateway by default communicates with printers through IPP.

If the printer is not supporting IPP or if the communication between the iPrint gateway and printers through IPP fails then the printer's attributes are retrieved using SNMP.

For more information, see Modifying the Printer’s Gateway Load Commands in OES 23.4: OES iPrint Administration Guide.

Email Printing with Gmail and O365

After Google enhanced their authentication, if you are providing Gmail ID in Email configuration, you must provide App Password (application specific password). For more information, see Global Email Settings in OES 23.4: iPrint Advanced Administration Guide

Logging Framework (log4j) Updated

For improved security, updated log4j to the latest version.

1.2.10 Domain Services for Windows (DSfW)

NAS Synology 7.x Support

The OES 23.4 server supports the NAS 7.x Synology version, which offers DirSync search capabilities and compatible attributes for all users and groups. DSfW has extended the support to DirSync search capabilities

Thus, the NAS server is able to fetch users and groups data from the server using DirSync search and DSfW returns data as per the latest requirement.

Samba 4.15 Support

The Samba version was updated from 4.10 to 4.15 to be compatible with SLES version of Samba and to resolve library conflict between base SLES and earlier SLES versions.

Additionally, Samba 4.15 supports important changes to security vulnerability.

1.2.11 NetWare Core Protocol (NCP)

Security Configuration Audit

A new audit log is initiated for tracking the operations for security configuration such as MFA and encryption for NCP connections. For tracking, the users must login through NCP connections.

1.2.12 Client for Open Enterprise Server

NCP Server Side Copy

Beginning with Client for Open Enterprise Server 2 SP7 (IR4) and later, the "OES Copy" functionality will take advantage of Open Enterprise Server capabilities to perform server-side copy operations. This capability will be available only if the source and destination paths specified in the “OES Copy” dialog are within the same volume, or for paths that represent distinct volumes within the same server.

When the supplied paths are determined to qualify for taking advantage of OES server-side copy capabilities, the files is copied using OES server-side copy NCPs. This will be more efficient than reading and writing the data through the Client for Open Enterprise Server workstation, and can also substantially increase the performance in scenarios where VPN or low-bandwidth networks are involved that would otherwise limit the data transfer rate.

For more information, see Client for Open Enterprise Server 2 SP7 Documentation (https://www.microfocus.com/documentation/client-for-open-enterprise-server/2-sp7/).

1.2.13 Storage Services File System (NSS)

Cache Devices

Cache devices (**cachedev**) are special block devices that are designed for hosting cache for the NSS storage pools. You can group the free storage space available in the fast storage devices to form the cache device. Adding partitions or more devices will allow you to expand the cache device even further.

For additional storage operations like building a pool, you can utilize cache device like a regular block device.

To configure and manage the cache devices, you must use the NLVM command-line utility. For more information, see NLVM Commands in OES 23.4: NLVM Reference.

NOTE: Currently this feature is available only on local devices and with 512-byte sector size devices.

Cache Enabled Pools

The NSS storage pools can have cache on a specific cache device in order to improve the IO performance. Three components constitute the Cache Enabled Pool: the cache, cache metadata, and data from the NSS pool. Cache and metadata are not accounted as part of the pool's space and hence they will not increase the available NSS pool's space.

Performance improvements are achieved by reading and writing blocks from the storage device with greater speed. The persistence nature of cache, keeps the cache warm across reboots too.

When a pool is created, the cache can be assigned to it and linked to it, or it can be enabled later.

For more information, see Cache Enabled Pools in OES 23.4: NSS File System Administration Guide for Linux.

NOTE: Currently this feature is available only on local pools and with 512-byte sector size devices.

1.2.14 DNS / DHCP

Configure Log-Level Attribute using Java Console

Beginning with OES 23.4, administrator can configure the log-level attribute using Java Management Console. During dynamic reconfiguration or `novell-named.service` restart, the DNS server detects the changes and reconfigures `novell-named` with log-level specified in Java Console. The log-level attribute changes are also saved in the `named.conf` file.

For more information, see Configuring Log-Level using Java Management Console in OES 23.4: DNS/DHCP Services for Linux Administration Guide.

1.2.15 Unchanged Components in OES 23.4

Besides branding and bug fixes, there are no other changes to the following components:

- Linux User Management (LUM)
- Business Continuity Clustering (BCC)
- OES FTP
- Storage Management Services (SMS)
- OES Cluster Services (NCS)
- VLOG
- Dynamic Storage Technology (DST)
- Micro Focus Subscription Management Tool (MFSMT)
- OES User Rights Map (NURM)
- Novell Remote Manager (NRM)

1.3 OES Entitlements

The following are the entitlement to all OES customers under maintenance:

- Filr Standard
- iPrint Desktop (Appliance)
- iPrint Advanced (Except mobile printing)
- Cluster services 2 node entitlement
- Micro Focus Kanaka for Mac
- IDM Bundle Edition
- NetIQ Self Service Password Reset as an indirect entitlement via their IDM BE entitlement
- Advanced Authentication Limited Edition

2 Service Issues

Additional tips are found in the troubleshooting sections of the OES service administration guides.

- Section 2.1, “OES Installation, Upgrade and Update,” on page 15
- Section 2.2, “Client for Open Enterprise Server,” on page 17
- Section 2.3, “Distributed File Services (DFS),” on page 18
- Section 2.4, “Business Continuity Clustering (BCC),” on page 20
- Section 2.5, “Cloud Integrated Storage (CIS),” on page 21
- Section 2.6, “DNS/DHCP Services,” on page 21
- Section 2.7, “Domain Services for Windows (DSfW),” on page 22
- Section 2.8, “eDirectory,” on page 23
- Section 2.9, “Identity Console,” on page 24
- Section 2.10, “iManager,” on page 24
- Section 2.11, “iPrint Advanced,” on page 25
- Section 2.12, “NetWare Core Protocol (NCP),” on page 25
- Section 2.13, “OES Cluster Services (NCS),” on page 25
- Section 2.14, “OES Remote Manager (NRM),” on page 26
- Section 2.15, “OES Storage Services (NSS),” on page 27
- Section 2.16, “OES User Rights Map (NURM),” on page 27
- Section 2.17, “Unified Management Console (UMC),” on page 27

2.1 OES Installation, Upgrade and Update

- Section 2.1.1, “Package Conflict Issue,” on page 15
- Section 2.1.2, “Channel Upgrade Issue,” on page 16
- Section 2.1.3, “Upgrade Issue in SUSE Xen Hypervisor Environment,” on page 16
- Section 2.1.4, “NCS and Upgrade Issue,” on page 17
- Section 2.1.5, “OES Server Registration to MFSMT Fails,” on page 17

2.1.1 Package Conflict Issue

During the OES upgrade, you may encounter package conflict issues related to PHP version 8. To resolve this issue, you must uninstall PHP version 7 and then proceed with the OES upgrade.

2.1.2 Channel Upgrade Issue

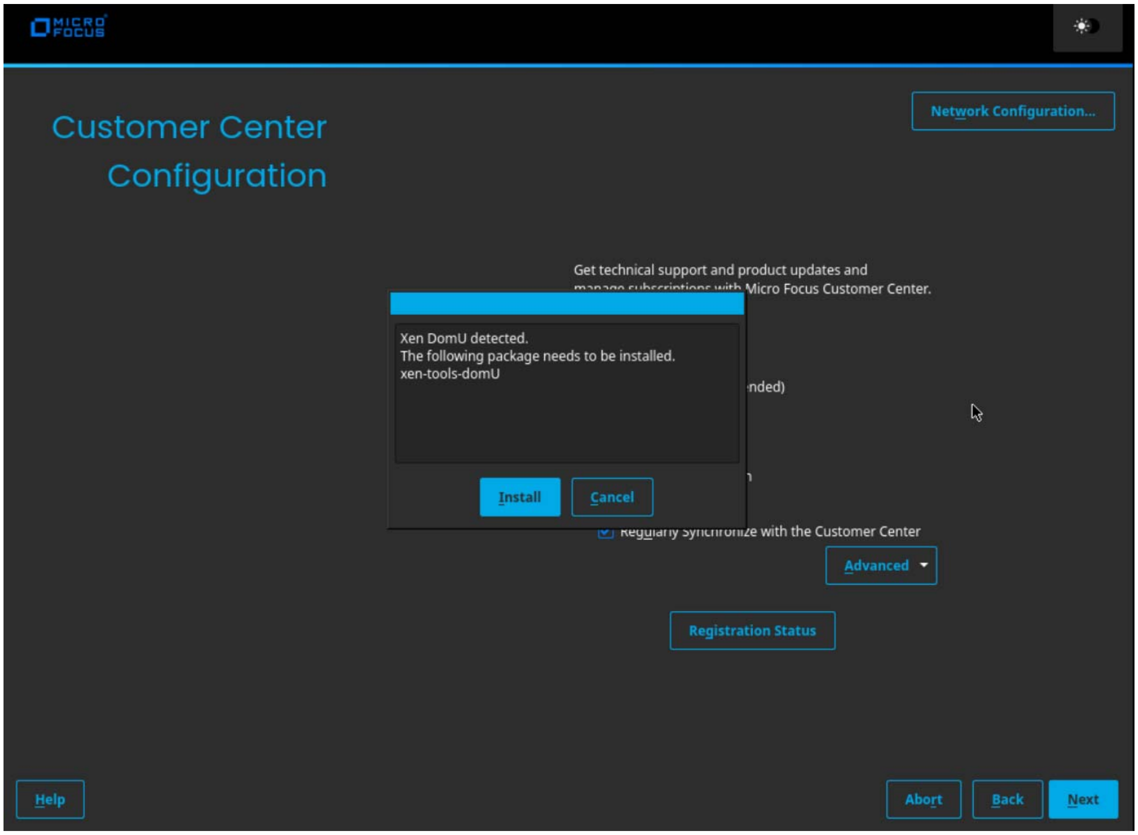
The value of "`SERVICE_CONFIGURED=`" in `/etc/sysconfig/novell/edir` is changed from "`yes`" to "`no`" by the "`yast2 channel-upgrade-oes`" command during the Channel Upgrade from OES 2023 to OES 23.4 using Zypper. This was resulting in an upgrade issue, which is now fixed in Update 5.1 OES 2023 Hotfix.

To avoid this issue, ensure that OES 2023 is updated with the latest patches from the channel before upgrading to OES 23.4.

2.1.3 Upgrade Issue in SUSE Xen Hypervisor Environment

If you are in a SUSE Xen Hypervisor environment and upgrading to OES 23.4, the upgrade fails. It is recommended to follow either one of the following workarounds:

- If you have already registered to customer center, you must **Cancel** the `xen-tools-domU` package installation to proceed with the upgrade process.



Customer Center Configuration

Get technical support and product updates and manage subscriptions with Micro Focus Customer Center.

Xen DomU detected.
The following package needs to be installed.
xen-tools-domU

☑ Regularly synchronize with the Customer Center

- If you have not registered to customer center, skip the registration to proceed with the upgrade process.

2.1.4 NCS and Upgrade Issue

When OES Cluster Services (NCS) and Business Continuity Clustering (BCC) are upgraded from OES 2023 to OES 23.4, NCS and BCC are not configured after the upgrade, hence NCS cluster and BCC peer clusters are not visible in the cluster view.

To resolve this issue, you must modify the administrator credentials or LDAP server settings that you assigned when you created the cluster. See, Changing the Administrator Credentials or LDAP Server IP Addresses for a Cluster in OES 23.4: OES Cluster Services for Linux Administration Guide.

2.1.5 OES Server Registration to MFSMT Fails

The registration of OES server to MFSMT fails with `ERROR: 500: Server error!`. This is because the SMT server is unable to identify the client IP address.

To avoid this issue, perform the following on the SMT Server:

1. Go to the file `/srv/www/perl-lib/SMT/Registration.pm`.
2. At line number 714, replace `$hostname = $r->connection()->remote_ip();` with `$hostname = $r->connection()->client_ip();` and save the file.
3. Restart the Apache service by using the command `systemctl restart apache2.service`.

2.2 Client for Open Enterprise Server

- Section 2.2.1, "On Enabling NCP Encryption Disable Send File Support," on page 17
- Section 2.2.2, "Accessing OES File Copy Utility in Windows Explorer Issue," on page 17
- Section 2.2.3, "OES File Copy Utility Notifies Incorrect File Size," on page 17
- Section 2.2.4, "OES File Copy Utility Fails for DFS Junction Volume," on page 18

2.2.1 On Enabling NCP Encryption Disable Send File Support

The send file support is not available when NCP encryption is set to `enable` or `enforce`. So ensure to set `SENDFILE_SUPPORT=0`, else the file and folder copy operations fail between:

- The mapped drives
- The mapped drives and local machine and vice versa

2.2.2 Accessing OES File Copy Utility in Windows Explorer Issue

If you right-click on any file or folder and select **OES Copy** from Windows Explorer, the **OES File Copy Utility** does not display the complete path of the selected file or folder. Instead, it only displays the drive name. Because of this issue, the performance of OES Copy utility is reduced.

2.2.3 OES File Copy Utility Notifies Incorrect File Size

For greater than 4 GB of data transfer, **OES File Copy: Copying Files** notification window displays file size as 41943003KB. **OES File Copy,** however, completes the data transfer with actual file size.

2.2.4 OES File Copy Utility Fails for DFS Junction Volume

OES File Copy utility works fine with all volumes expect DFS junction volume.

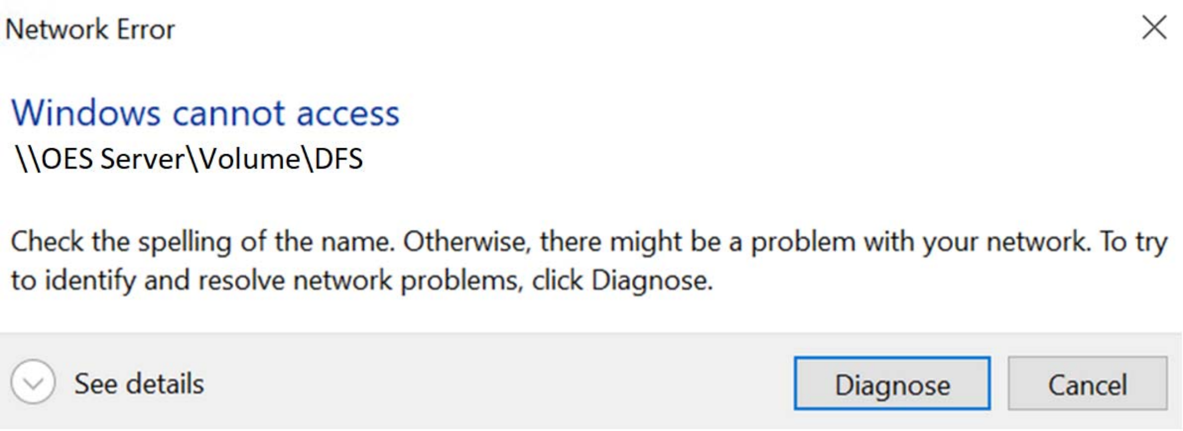
2.3 Distributed File Services (DFS)

- Section 2.3.1, “Windows Cannot Access Error,” on page 18
- Section 2.3.2, “CIFS eDir User can Access Non-OES Windows Target DFS Junction,” on page 18
- Section 2.3.3, “Non-OES Target Validation Errors,” on page 19
- Section 2.3.4, “NCP Clients Issues,” on page 19
- Section 2.3.5, “iManager Issues,” on page 19
- Section 2.3.6, “RME must be Configured for DFS Junction Pointing to Multiple Targets,” on page 19
- Section 2.3.7, “DFS Junction Pointing to Non-OES Target using Windows Domain Name,” on page 20
- Section 2.3.8, “DFSTOOL Command Errors,” on page 20

2.3.1 Windows Cannot Access Error

A permission denied error will appear for the user if Windows SMB Share or Windows Server are not available, or no trustee rights are available for the Windows SMB Share.

Figure 2-1 *Error Message*



Network Error

Windows cannot access
\\OES Server\Volume\DFS

Check the spelling of the name. Otherwise, there might be a problem with your network. To try to identify and resolve network problems, click Diagnose.

2.3.2 CIFS eDir User can Access Non-OES Windows Target DFS Junction

If the Active Directory administrator permissions are granted to Windows share, the CIFS eDirectory user can access the DFS junction on the non-OES Windows target DFS junction.

2.3.3 Non-OES Target Validation Errors

By default, `dfstool` uses anonymous login to validate the non-OES SMB share without prompting the user for any credentials on the command line. The `dfstool` does not check the path for the existence of the path from the share. If the anonymous login is disabled on the server hosting the target then junction creation or modification might fail.

The **`i`** option can be used to establish the non-OES junction without verifying the existence of the target server or share:

-
  ```
  dfstool -c /media/nss/VOL1/dir1/junc1 -t target_server_or_ip_address/
  share_name/path_to_target_folder -T non-oes -i
  ```

  (or)

  ```
  dfstool -c /media/nss/VOL1/dir1/junc1 -t target_server_or_ip_address/
  share_name/path_to_target_folder -T non-oes --ignore-targetpath-check
  ```

-
  ```
  dfstool -m /media/nss/VOL1/dir1/junc1 -t target_server_or_ip_address/
  share_name/path_to_target_folder -T non-oes -i
  ```

  (or)

  ```
  dfstool -m /media/nss/VOL1/dir1/junc1 -t target_server_or_ip_address/
  share_name/path_to_target_folder -T non-oes --ignore-targetpath-check
  ```

2.3.4 NCP Clients Issues

- NCP client does not list non-OES targets.
- For DFS junction, the NCP client is unable to list all multiple targets. In a failover scenario, the NCP client cannot use the other target if one of the targets is unavailable as the NCP clients always points to the first target path.

2.3.5 iManager Issues

- iManager is unable to list DFS junctions that point to multiple targets.
- If an NSS volume has both OES and a non-OES junction, iManager junction scan lists only OES junctions. So, to view non-OES junctions, you must use dfstool.
- When browsing through the NSS volume for modifying or deleting DFS junction, iManager does not list non-OES Windows junction target and only displays the OES junction.

2.3.6 RME must be Configured for DFS Junction Pointing to Multiple Targets

Cluster migrating a resource (which has a first target path) to another server (which has a second target path) followed by "vldb repair" would result in only one active target path until the user configures Resource Mutual Exclusion (RME).

2.3.7 DFS Junction Pointing to Non-OES Target using Windows Domain Name

- If you have configured Windows DFS root namespace, you can create a DFS junction pointing to DFS root namespace or folder under the root namespace.
- If you have not configured DFS Root Namespace, you cannot access the DFS junction target.

2.3.8 DFSTOOL Command Errors

- Scan or list junction is unable to list DFS junctions that point to multiple targets.
- Scan junction fails to work on non-replica VLDB servers and throws an error.
- dfstool does not validate the special characters ($$, $!) appended to the share name and creates junction successfully.
- dfstool throws an encryption issue even though the junction is successfully created when creating a junction with Netapp shares using the -A option.
- When using DFS Namespace to generate a non-OES junction, dfstool incorrectly lists the non-OES junction target path because DFS Namespace is appended before the SMB target share.

Junction Name	Source Server	Source Path	Target Server	Target Path	Management Context	Status
junc1	OESserver	Vol1:/ nonoes/	Windows_domain	DFSnamespace:/ Winshare1/	*NA*	Available
junc2	OESserver	Vol1:/ nonoes/	Windows_domain	DFSnamespace:/ Winshare1/dir1	*NA*	Available

2.4 Business Continuity Clustering (BCC)

- Section 2.4.1, “BCC Connections Fail on Enabling only TLS v1.3,” on page 20
- Section 2.4.2, “Cannot Add a New Volume on a BCC Migrated NSS Pool,” on page 21
- Section 2.4.3, “Multiple-Tree Configurations Are Not Supported,” on page 21

2.4.1 BCC Connections Fail on Enabling only TLS v1.3

In OES 23.4 with BCC installed and configured, enabling only the TLS v1.3 protocol in the `sfcb.cfg` file makes the BCC cluster connections to break. To avoid this and maintain stable connections, enable TLS v1.2 as well.

2.4.2 Cannot Add a New Volume on a BCC Migrated NSS Pool

When a BCC-enabled pool cluster resource is brought online in a peer cluster other than where it was originally created, you cannot add a new volume on the pool. The volume is created on the disk, but the Volume object fails to be added to Novell eDirectory with `Error 613: Error adding volume to NDS`.

We recommend that you create only one volume per pool cluster resource. If you need to add a volume on a BCC-enabled pool cluster resource, you must BCC-migrate the resource back to the peer cluster where the pool was originally created.

In some disaster situations, it is possible that the pool cluster resource has been permanently relocated to the current peer cluster. To cluster-enable the pool in its current cluster, see Permanently Relocating a Cluster Resource to a Peer Cluster in the OES 23.4: BCC Administration Guide.

2.4.3 Multiple-Tree Configurations Are Not Supported

In the BCC 2.6 release, multiple-tree configurations of business continuity clusters are not supported. All peer clusters must reside in the same tree.

2.5 Cloud Integrated Storage (CIS)

- Section 2.5.1, “CIS configuration Fails if the CIS pattern is Selected During OES installation with BIOS Firmware,” on page 21

2.5.1 CIS configuration Fails if the CIS pattern is Selected During OES installation with BIOS Firmware

During the installation, if CIS is combined with other services, you have to restart the server before configuring CIS.

2.6 DNS/DHCP Services

- Section 2.6.1, “DHCP Pattern Conflict,” on page 21

2.6.1 DHCP Pattern Conflict

When you select DHCP pattern post installation, a pattern conflict message is displayed. To continue, select the first option.

```
1. Following actions will be done.
install novell-oes-dhcp-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
install novell-oes-dhcp-relay-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
install novell-oes-dhcp-server-4.3.3_OES-3.68.x86_64 (with vendor change)
 SUSE LLC <https://www.suse.com/>  -->  Novell, Inc.
 deinstallation of dhcp-client-4.3.3-10.14.1.x86_64
```

2.7 Domain Services for Windows (DSfW)

- Section 2.7.1, “Cannot Configure UMC on DSfW Server,” on page 22
- Section 2.7.2, “Cannot Create Samba Shares,” on page 22
- Section 2.7.3, “CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers,” on page 22
- Section 2.7.4, “Workaround for DSFW Name-Mapped Tree,” on page 22
- Section 2.7.5, “Mixed Mode Configuration is not Supported,” on page 23
- Section 2.7.6, “DSfW Interoperability Issues,” on page 23

2.7.1 Cannot Configure UMC on DSfW Server

UMC configuration on DSfW Domain Controllers (FRD, ADC, or CDC) fail in Name-Mapped and Non Name-mapped DSfW setup. UMC is unable to detect the existing UMC server in the same tree.

2.7.2 Cannot Create Samba Shares

The Samba shares cannot be created in iManager because the NCP Server object fails to load during the process. However Samba shares can be created in the `smb.conf` file.

2.7.3 CIS Pattern Conflict in DSfW Name-Mapped/Non-Name-Mapped Servers

CIS pattern cannot be installed on Name-Mapped and Non-Name-Mapped DSfW servers.

2.7.4 Workaround for DSFW Name-Mapped Tree

On a Name-Mapped deployment, CIS is installed on the eDirectory server and DSfW is installed on a partitioned container. Dashboard is not able to fetch DSfW server details since CIS and DSfW are in different domains.

Workaround: DSfW domain DNS is added as a primary DNS in the eDirectory server where CIS is installed. With this change CIS resolves DSfW domain and started fetching DSFW server details.

2.7.5 Mixed Mode Configuration is not Supported

Beginning with OES 2018 SP1, the DSfW domain controllers having OES 2018 SP1 or later and those having earlier OES versions cannot coexist in a forest. This is because of the functional incompatibility between the updated Kerberos version in OES 2018 SP1 and the Kerberos version in OES 2018 and earlier. All the DSfW servers in a forest must be on the same OES version and on the same patch level.

2.7.6 DSfW Interoperability Issues

IMPORTANT: The following list is provided for your convenience. Do not consider the list as complete. Be sure to consult the documentation for your other OpenText products for information on interoperability issues with DSfW.

ZENworks Endpoint Security Management 3.5

On an OES 2018 server with DSfW installed, the Endpoint Security Management utility fails on all DSfW server ports.

OpenText has no current plans to change this.

2.8 eDirectory

The following are the known OES-specific eDirectory issues. For general eDirectory issues, refer to the eDirectory documentation website.

- Section 2.8.1, “eDirectory Features Not Supported in OES,” on page 23
- Section 2.8.2, “eDirectory Not Restarting Automatically,” on page 24

2.8.1 eDirectory Features Not Supported in OES

The following eDirectory features are not supported:

- SUITE B

  For more information, see Configuring eDirectory in Suite B Mode in the NetIQ eDirectory Administration Guide.
- Enhanced Background Authentication (EBA)
- FIPS

NOTE: With OES 2018 SP1 or earlier, along with these eDirectory features, creation of AES 128-bit tree key or 256-bit tree key is also not supported.

2.8.2 eDirectory Not Restarting Automatically

After a system crash or power failure, eDirectory services (`ndsd`) might not automatically start in some situations.

To start eDirectory again:

1. Delete the `/var/opt/novell/eDirectory/data/ndsd.pid` file.
2. At a terminal prompt, enter `systemctl start ndsd.service`

2.9 Identity Console

The following are the issues with the standalone Identity Console installed on OES 2023:

- **Adding replica objects:** Unable to add OES server replica objects using the Partition Management plugin.
- **Modifying LDAP settings:** Identity Console does not accept modifications to the LDAP settings (TLSv1.2, TLSv1.x, sslv3, and so on). The modifications made through iManager are also not reflected on Identity Console.
- **eDirectory Group attributes:** Identity Console fails to list the valued attributes for the eDirectory groups that are synced to AD server container through IDM AD driver. However, for the same groups, the attributes are listed in iManager.
- **Login to iPrint portal:** Login to iPrint Print Portal and Release Portal fails with username, if the user is created using Identity Console.
- **Modifying User or Group:** The modifications made to the users and groups using Identity Console does not get saved.
- **Browsing eDirectory context:** The eDirectory context and sub context cannot be browsed from the context field.
- **Creating home directory:** When creating an OES eDirectory user using the User Management plugin, home directory creation inside the NSS volume fails.
- **Setting object value:** For a newly created NSS volume, the value for the object LinuxNCPMountPoint is neither set by default nor can be set by selecting it from the drop-down list. However, it can be set by manually entering the value.
- **Browsing folders:** The deep level folders created under an eDirectory object cannot be browsed from the tree view.

2.10 iManager

- Section 2.10.1, “Uninstalling Plugins from iManager 3.2.6 Fails,” on page 25
- Section 2.10.2, “Updating and Uninstalling Plugins using iManager Post-OES Upgrade Fails,” on page 25
- Section 2.10.3, “Issues with OES 2023 Cluster Plugin,” on page 25

2.10.1 Uninstalling Plugins from iManager 3.2.6 Fails

After installing the iManager 3.2.6 plugins using YaST during the installation process, uninstalling (**iManager > Configure > Plug-in-Installation > Installed Novell Plug-in Modules**) the iManager 3.2.6 plugins fails. However, installation and uninstallation of new plugins can be done through iManager.

2.10.2 Updating and Uninstalling Plugins using iManager Post-OES Upgrade Fails

During upgrade to OES 2023, in the iManager configuration page, updating and uninstalling the plugins using iManager 3.2.6 fails. This issue is observed only on those plugins that were installed with the iManager 3.2.5 or earlier before upgrading to OES 2023. However, you can install new plugins from the **Available Novell Plug-in modules** in iManager 3.2.6 after upgrade to OES 2023. You can uninstall the plug-in as long as it is installed in iManager 3.2.6, either via the iManager web-interface or in YaST during the upgrade workflow.

2.10.3 Issues with OES 2023 Cluster Plugin

If you are using a standalone iManager workstation, it is recommended not to upgrade to OES 2023 cluster plugin (`ncsmgmt.npm`). cluster plugin. There are a few issues with the latest cluster plugin such as missing buttons and empty tabs.

2.11 iPrint Advanced

- Section 2.11.1, "Documents with SmartArt Graphics or Tables," on page 25

2.11.1 Documents with SmartArt Graphics or Tables

Printing documents with SmartArt graphics or tables may impact the quality of the printout. It is recommended to test the quality of printouts before deploying in a production environment.

2.12 NetWare Core Protocol (NCP)

- Section 2.12.1, "On Enabling NCP Encryption Disable Send File Support," on page 25

2.12.1 On Enabling NCP Encryption Disable Send File Support

The send file support is not available when NCP encryption is set to `enable` or `enforce`. So any setting to `SENDFILE_SUPPORT` is ineffective when encryption is set to `enable` or `enforce`.

2.13 OES Cluster Services (NCS)

- Section 2.13.1, "Cluster Node Crashing Issue," on page 26
- Section 2.13.2, "Cluster Enabled Linux Volume Creation Failure," on page 26

2.13.1 Cluster Node Crashing Issue

If you stop the cluster service on a cluster node while running **Update 2 OES 2023 Patch** or the latest kernel version, the cluster node will crash. To avoid the cluster node from crashing, follow the below steps:

1 Log in to the node as the root user, then open a terminal console.

2 Disable the Novell Cluster Service.

```
systemctl disable novell-ncs.service
```

3 Remove the node from the cluster.

```
cluster leave
```

4 Ensure that all cluster resources are moved to other cluster node.

5 Stop the Novell Cluster Service.

```
systemctl stop novell-ncs.service
```

NOTE: Stopping the Novell Cluster Service leads to cluster node crash.

6 Reboot the server.

7 Enable the Novell Cluster Service on the cluster node.

```
systemctl enable novell-ncs.service
```

8 Apply the **Update 3 OES 2023 Patch** on the cluster node.

```
zypper patch
```

9 Reboot the server.

2.13.2 Cluster Enabled Linux Volume Creation Failure

The creation of cluster enabled Linux volume fails with `Error 23384`. This is because of the deprecation of `clvmd` support for `lvm` commands on SLES. Cluster enabled lvm2 volume on OES 2018 SP3 or earlier goes comatose after upgrade to OES 2023.

2.14 OES Remote Manager (NRM)

- Section 2.14.1, “Newly Installed or Upgrade Issue,” on page 26
- Section 2.14.2, “Nagios Service,” on page 27
- Section 2.14.3, “Unable to Perform Group Operations,” on page 27

2.14.1 Newly Installed or Upgrade Issue

The status of the `novell-httpkstd` service may be "**activating**" instead of "**active**" in newly installed or upgraded systems.

Workaround:

1. Kill the `novell-httpkstd` service.

```
systemctl kill novell-httpstkd.service
```

2. Restart the novell-httpkstd service.

   ```
   systemctl restart novell-httpstkd.service
   ```

2.14.2 Nagios Service

The Nagios service does not come up automatically. The service is not enabled by default. You have to manually enable it using the command `systemctl enable --now nagios.service`.

2.14.3 Unable to Perform Group Operations

The group operations cannot be performed using **Use Group Operations** in NRM on OES 2023.

2.15 OES Storage Services (NSS)

- Section 2.15.1, “RAID 5 Issues,” on page 27

2.15.1 RAID 5 Issues

Some issues can occur when you lose a device in an NSS software RAID 5 device, or when you expand an NSS software RAID 5 device. The following issues happen intermittently:

When a segment is missing in an NSS RAID 5 because of a device failure, the pool might hang until the device driver reports the error, and then the RAID continues. The hang time depends on the underlying device driver timeout conditions. For iSCSI devices, this includes iSCSI driver timeout. For extended hangs, the pool might also get deactivated.

2.16 OES User Rights Map (NURM)

- Section 2.16.1, “Unable to Apply Map Rights Using the IDM User Map,” on page 27

2.16.1 Unable to Apply Map Rights Using the IDM User Map

The utility `user-rights-map` cannot be used for mapping the rights in NURM by using the user map created from IDM.

2.17 Unified Management Console (UMC)

- Section 2.17.1, “UMC Configuration,” on page 27

2.17.1 UMC Configuration

Configuring UMC on OES 2023 removes any existing Postgres database configuration. Therefore, if an OES server is upgraded from OES 2018 SP3 or earlier on which the Postgres database is already configured and is being used by any of the customer applications, it is recommended not to configure UMC on such an upgraded OES 2023 server.

A Verifying the Integrity of the Downloaded Files

To ensure a successful installation, you must compare the sha256sum value of the downloaded file with the corresponding checksum value.

1. Login to Software Licenses and Downloads (SLD) (https://sld.microfocus.com/mysoftware/index) website or if you don’t have a Micro Focus account, create an account.
2. Click **Downloads** and select the product as **Open Enterprise Server 23.4**, product name depending on your license type and version as **23.4**.
3. In the **Action** column, mouseover **More Details to view** the .iso name and checksum value.
4. Verify the integrity of each downloaded file:

- On a Linux system at the shell prompt, enter the following command:

  `sha256sum` *filename*

  where *filename* is the name of the `.iso` file you are verifying.
- On a Windows system, open a PowerShell command and enter the following command:

  `Get-FileHash` *filename*

  where *filename* is the name of the file you are verifying.

B Deprecated Components and Services

- ## iManager

  Beginning with OES 23.4, iManager is deprecated. Unified Management Console (UMC) provides customized access to network administration utilities and content from virtually anywhere using the Internet and a web browser similar to iManager. For more information about UMC, see OES 23.4: Unified Management Console.

- ## Apple Filing Protocol (AFP)

  Beginning with OES 2023, AFP is deprecated. New installations of OES 2023 will not include pattern to install AFP. OpenText offers OES CIFS as an alternative to AFP.

- ## Service Proxy

  Beginning with OES 2023, service proxy is being deprecated on a new server in favor of common-proxy and will not be supported in the future releases. If any service is configured with service-specific proxy users in the earlier versions of OES, then an upgrade to the OES 2018 SP1 or later server moves the service to use a common proxy user.

- ## ShadowFS

  ShadowFS uses FUSE to create a local mount point for merged view of each DST shadow volume pair. Beginning with OES 2023, ShadowFS support is being deprecated and will not be supported. If you are using or taking advantage of ShadowFS, then request you to email us at oes@microfocus.com

- ## Ganglia Module in OES Remote Manager

  Beginning with OES 2023, the support for Ganglia is discontinued. Therefore, the **Server Health Values** link that was used to monitor the health of the server is no more available in OES Remote Manager.

- ## NetStorage

  Beginning with OES 2023, NetStorage is deprecated. New installations of OES 2023 will not include pattern to install NetStorage. OpenText offers Filr as an alternative to NetStorage. Although, Filr is a separate product, its Standard version is offered as an entitlement to OES customers. For more information about Filr, see Filr Overview (https://www.microfocus.com/en-us/products/filr/overview).

- ## Novell Samba

  Beginning with OES 2018 SP1, Novell Samba is deprecated. New installations of OES 2018 SP1 will not include pattern to install Novell Samba.

If you are upgrading to OES 2018 SP1 from an earlier OES version that includes Novell Samba, the package and configuration will be removed during the upgrade process. It is recommended to install and use Novell CIFS to access the data that was earlier accessed from Samba shares. For more information, see Understanding the Implications of Novell Samba Currently Installed on the Server in the OES 2018 SP3: Installation Guide.

- **Service Migration**

  Beginning with OES 2018, service migration from supported OES platforms to latest OES platform is no longer supported except for the following services:

  - iPrint
  - File system data
  - Transfer ID

  Beginning with OES 2023, building and bundling of the unsupported service plugins are also discontinued.

- **iFolder**

  Beginning with OES 2018, iFolder is deprecated. New installations of OES 2018 will not include pattern to install iFolder.

  If you are upgrading to OES 2018 or later from an OES 2015 SP1 or earlier server that includes iFolder, the package will not be accessible on the OES 2018 or later server. However, the iManager plug-in is still available post upgrade, and you can use them to manage servers prior to OES 2018.

- **Archive and Version Service (AV) and QuickFinder**

  Beginning with OES 2015, Archive and Version Services (AV) and QuickFinder services are deprecated. New installations or upgrade to OES 2015 and later will not include patterns to install these components.

  If you are upgrading to OES 2015 or later from an OES 11 SP3 or earlier server that includes the Archive and Versioning Services (AV) and QuickFinder, these packages and the associated data will not be accessible on the OES 2015 or later server. However, the iManager plug-ins for AV and QuickFinder are still available post upgrade to OES 2015, OES 2015 SP1, or OES 2018 and you can use them to manage servers prior to OES 2015.

  Beginning with OES 2018 SP1, the iManager plug-ins for AV and QuickFinder are obsolete.