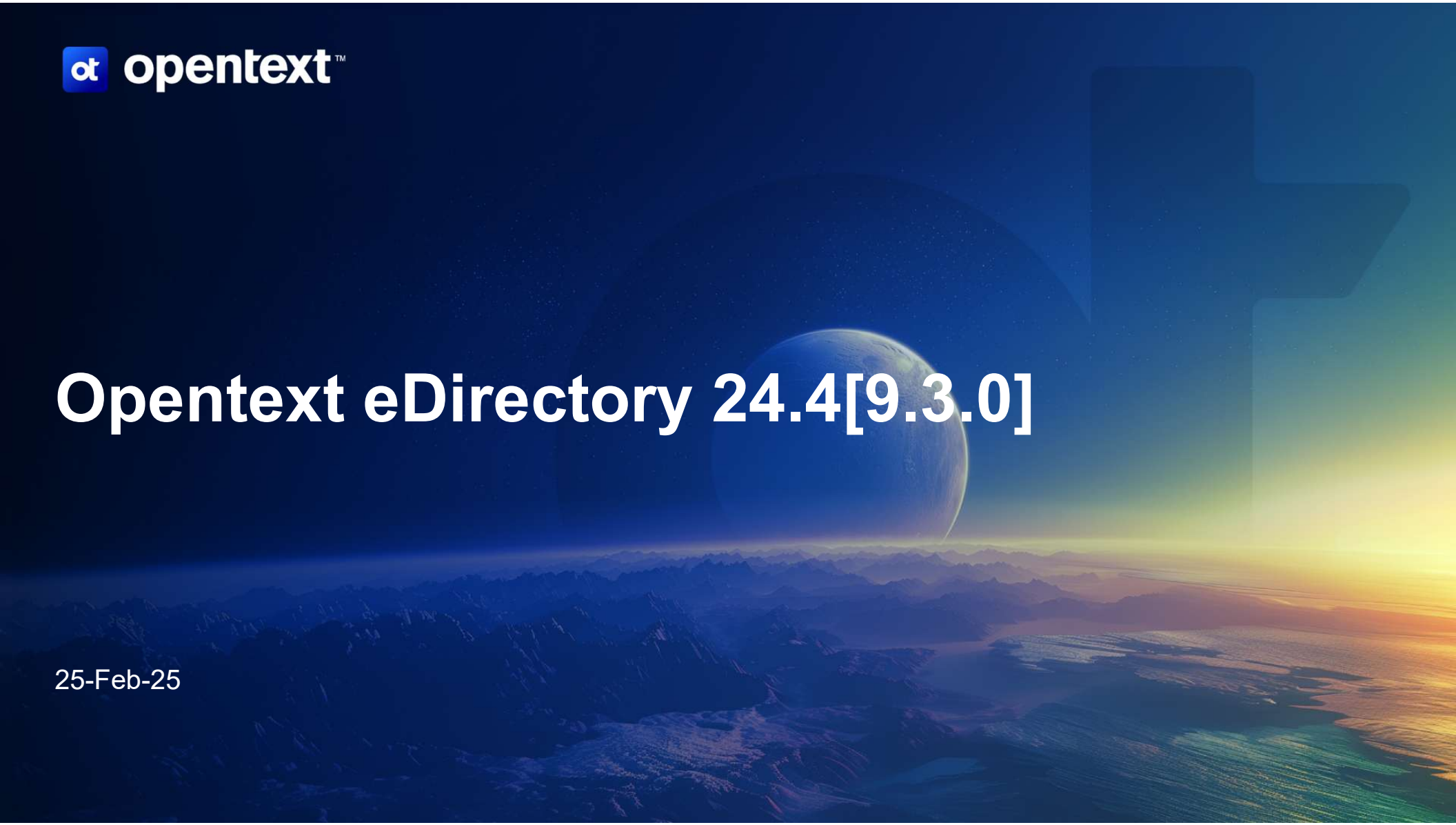

opentext™
Opentext eDirectory 24.4[9.3.0]
25-Feb-25

Agenda

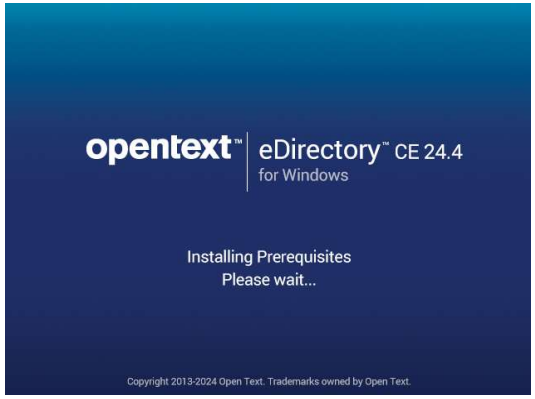
- What's New?
- Backward Compatibility
- The Future

eDirectory 24.4 –What's New?

- **Migrated from OpenSSL 1.0.2 [extended support] to OpenSSL 3.0.15**
- **TLS 1.3 /1.2 Support**
  - Cipher suites have been updated to align with OpenSSL 3.0 and include the following TLS 1.3 Ciphers suites:
    - TLS_AES_256_GCM_SHA384.
    - TLS_CHACHA20_POLY1305_SHA256 (non-FIPS only).
    - TLS_AES_128_GCM_SHA256.
    - TLS 1.2 Ciphers continue with a mix of AES and RSA encryption options.
- **FIPS Uniformity**: NICI configuration file- nici64.cfg becomes the reference point for enabling TLS FIPS and NICI FIPS

eDirectory 24.4 –What's New?

- **RSA Certificate and Encryption Algorithms**
  - RSA certificates with key sizes of 512, 768, or 1024 bits and SHA-1 Certificates are supported only in Non FIPS mode
  - RSA certificates with key sizes of 2048 bit and above, SHA-256 is the minimum supported configuration in FIPS mode
- **NICI Tree Key**
  - eDirectory 24.4 automatically creates AES 256-bit tree key for fresh install.
- **Opentext Rebranding and Versioning**



Backward Compatibility

- EBA Bridge Patch

Version	EBA Enabled	Bridge pack Required
9.2.8, 9.2.9	Yes	Yes
Below 9.2.8	Yes	Yes, Post upgrade to 9.2.8/9.2.9
All version	No	No

- Handling NMAS Methods-Post Upgrade

Single-Server Environment:	Multi-server Environment
NMAS Schema extension is required for Windows. This has been taken care in Linux and Docker as part of the installer.	In a mixed-version eDirectory setup, add the NMAS method to 9.2.9 servers before applying it to 9.3.0 servers for compatibility.

- Identity Manager 24.4[4.10] Compatible with eDirectory 24.4
- IdentityConsole 24.4[1.9.0] supports eDirectory 24.4 and lower versions

The Future

- EBA- CA Certificate renewal / repair mechanism.
- Improved Adoption of OpenSSL 3.0
  - SHA 256 or later
  - SHA1 will no longer be supported
  - RC-2-40, DES, 3DES will no longer be supported
- IPV6 support

Cipher Support eDirectory 24.4- Annexure 1

- TLS_AES_256_GCM_SHA384 TLSv1.3
- TLS_CHACHA20_POLY1305_SHA256 TLSv1.3[Non FIPS Only]
- TLS_AES_128_GCM_SHA256 TLSv1.3
- ECDHE-ECDSA-AES256-GCM-SHA384 TLSv1.2
- ECDHE-RSA-AES256-GCM-SHA384 TLSv1.2
- ECDHE-ECDSA-CHACHA20-POLY1305 TLSv1.2
- ECDHE-RSA-CHACHA20-POLY1305 TLSv1.2[Non FIPS Only]
- ECDHE-ECDSA-AES128-GCM-SHA256 TLSv1.2
- ECDHE-RSA-AES128-GCM-SHA256 TLSv1.2
- ECDHE-ECDSA-AES256-SHA384 TLSv1.2
- ECDHE-RSA-AES256-SHA384 TLSv1.2
- ECDHE-ECDSA-AES128-SHA256 TLSv1.2
- ECDHE-RSA-AES128-SHA256 TLSv1.2
- AES256-GCM-SHA384 TLSv1.2
- AES128-GCM-SHA256 TLSv1.2
- AES256-SHA256 TLSv1.2
- AES128-SHA256 TLSv1.2


opentext™
Thank you