# Planen Sie eine Datenmigration

XCP

NetApp
March 14, 2024

This PDF was generated from https://docs.netapp.com/de-de/xcp/xcp-plan-nfs-data-migration.html on March 14, 2024. Always check docs.netapp.com for the latest.

# Inhalt

Planen Sie eine Datenmigration . . . 1
Planen Sie NFS-Datenmigration . . . 1
Planen Sie die SMB-Datenmigration . . . 2
Planung der HDFS-Datenmigration . . . 2
Planen Sie die Verwendung von Dateianalysen . . . 3
Filter . . . 16
Protokollierung für NFS und SMB (optional) . . . 16

# Planen Sie eine Datenmigration

Die Migration kann über die Befehlszeilenschnittstelle oder die GUI von Dateianalysen geplant werden.

Planen Sie die Migration mit folgenden Befehlen:

- Anzeigen
- Scannen

Verwenden Sie die Dateianalyse, um die Statistiken für Exporte und Freigaben zu visualisieren.

# Planen Sie NFS-Datenmigration

Planen Sie Ihre NFS-Datenmigrationen.

## Anzeigen

Der `show` Der Befehl fragt die RPC-Dienste und NFS-Exporte von einem oder mehreren Speicherservern ab. Der Befehl listet die verfügbaren Dienste und Exporte mit der verwendeten und freien Kapazität jedes Exports auf, gefolgt von den Stammattributen jedes Exports.

**Beispiel:**

- `xcp show <NFS file server IP/FQDN>`
- `xcp show nfs_server01.netapp.com`

Laufen `xcp help show` Entnehmen.

## Scannen

Der `scan` Befehl scannt rekursiv die gesamten von der Quelle exportierten NFSv3-Pfade und druckt die Statistiken der Dateistruktur am Ende des Scans. NetApp empfiehlt, während des Scan-Vorgangs die Quell-NFS-Export-Mounts in den schreibgeschützten Modus zu versetzen.

> Wenn ein Datei- oder Verzeichnisname nicht-UTF-8-Zeichen enthält, werden diese Zeichen in das UTF-8-Format konvertiert und beim Ausführen des angezeigt `xcp-scan` Befehl. Abhängig von der Übersetzung von der Quellcodierung nach UTF-8 werden die Zeichen möglicherweise nicht wie erwartet angezeigt.

**Beispiel:**

- `xcp scan NFS [server:/export path | file:// ]`
- `xcp scan nfs_server01.netapp.com:/export1`
- `xcp scan file:///mnt/nfs-source`

Laufen `xcp help scan` Entnehmen.

Verwenden Sie optional die Dateianalyse, um die Ergebnisse grafisch anzuzeigen.

# Planen Sie die SMB-Datenmigration

Planen Sie Ihre SMB-Datenmigrationen.

## Anzeigen

Der `show` Der Befehl zeigt alle auf dem Server verfügbaren SMB-Freigaben mit den verfügbaren Berechtigungen und dem verfügbaren Speicherplatz an. Beispiel:

- `xcp show \\<SMB file server IP/FQDN>`
- `xcp show smb_server01.netapp.com`

Laufen `xcp help show` Entnehmen.

## Scannen

Der `scan` Befehl scannt rekursiv die gesamte SMB-Freigabe und listet alle Dateien am Ende des Scans auf.

> Während des Scanvorgangs können Sie das verwenden `-preserve-atime` Flagge mit dem `scan` Befehl zum Erhalt der Zugriffszeit an der Quelle .

**Beispiel:**

- `xcp scan \\SMB server\share1`
- `xcp scan smb_server01.netapp.com:/share1`

Laufen `xcp help scan` Entnehmen.

Verwenden Sie optional die Dateianalyse, um die Ergebnisse grafisch anzuzeigen.

# Planung der HDFS-Datenmigration

Planen Sie Ihre HDFS-Datenmigrationen.

## Scannen

Der `scan` Befehl scannt rekursiv die gesamten Quellpfade und druckt die Statistiken für die Dateistruktur am Ende des Scans.

- `xcp scan HDFS [hdfs://<hdfs mounted path> ]`
- `xcp scan hdfs:///demo/user1`
- `xcp scan s3://my-bucket`
- `xcp scan -s3.profile <s3 profile name> -s3.endpoint <endpoint-url> s3://my-bucket`

Laufen `xcp help scan` Entnehmen.

# Planen Sie die Verwendung von Dateianalysen

## Planen Sie Ihre Datenmigration

Planen Sie die Datenmigration mit Dateianalysen.

> XCP ist eine CLI, während File Analytics eine GUI hat.

### Übersicht

XCP-Dateianalysen erfasst Daten von NFS- oder SMB-Hosts über die XCP-Scan-API. Diese Daten werden dann in der XCP-Dateianalyse-GUI angezeigt. An der XCP-Dateianalyse sind drei Hauptkomponenten beteiligt:

- XCP-Dienst
- Dateianalyse-Datenbank
- Dateianalyse-GUI zum Managen und Anzeigen von Daten

Die Bereitstellungsmethode für XCP-Dateianalyselösungen hängt von der erforderlichen Lösung ab:

- Bereitstellung von XCP-Dateianalyselösungen für NFS-Dateisysteme:
  - Sie können die GUI, die Datenbank und den XCP-Service für Dateianalysen auf demselben Linux-Host bereitstellen.
- Bereitstellen von XCP-Dateianalyselösungen für SMB-Dateisysteme: Sie müssen die GUI und die Datenbank der Dateianalyse auf einem Linux-Host bereitstellen und den XCP-Dienst auf einem Windows-Host bereitstellen.

## Öffnen Sie Dateianalyse

Die Dateianalyse bietet eine grafische Ansicht der Scanergebnisse.

### Melden Sie sich bei der GUI von File Analytics an

Die GUI von XCP File Analytics bietet ein Dashboard mit Diagrammen zur Visualisierung von Dateianalysen. Die XCP-Dateianalyse-GUI ist aktiviert, wenn Sie XCP auf einem Linux-Rechner konfigurieren.

> Informationen zum Überprüfen der unterstützten Browser für den Zugriff auf Dateianalyse finden Sie im "NetApp IMT".

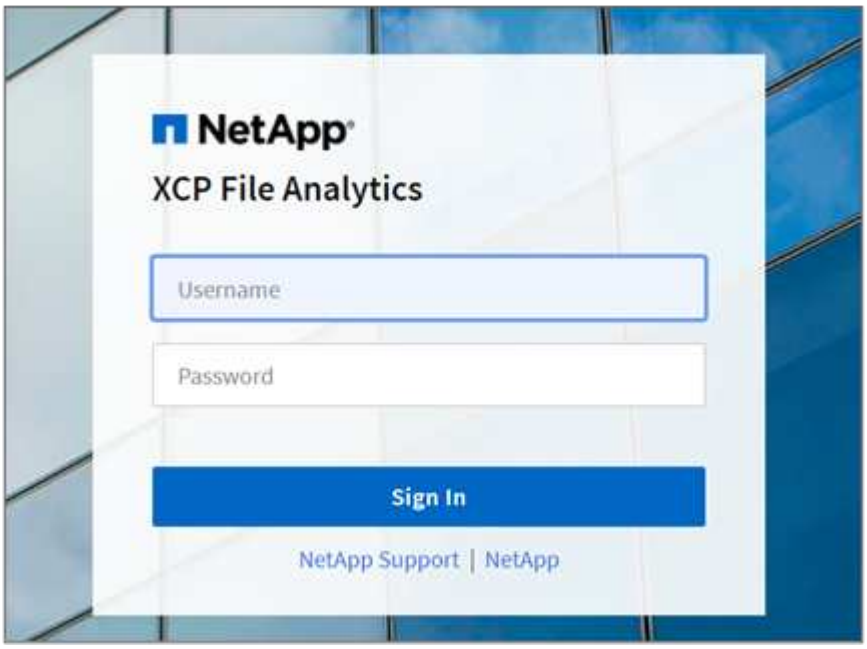
#### Schritte

1. Verwenden Sie den Link `https://<IP address of linux machine>/xcp` Um auf die GUI zur Dateianalyse zuzugreifen. Akzeptieren Sie bei entsprechender Aufforderung das Sicherheitszertifikat:
   a. Wählen Sie unter der Datenschutzerklärung **Erweitert** aus.
   b. Wählen Sie **Weiter mit `<IP address of linux machine>`** Link.
2. Melden Sie sich in der GUI für Dateianalysen an.

   Es gibt zwei Möglichkeiten, sich bei der GUI für Dateianalysen anzumelden:

**Melden Sie sich mit den Benutzeranmeldeinformationen an**

a. Melden Sie sich bei der GUI mit den Benutzeranmeldeinformationen an, die Sie bei der Installation von File Analytics erhalten haben.




b. Ändern Sie optional das Passwort in Ihr eigenes Passwort.

   Wenn Sie das bei der Installation erhaltene Passwort in Ihr eigenes Passwort ändern möchten, wählen Sie das Benutzersymbol und dann **Passwort ändern**.

   Ihr neues Passwort muss mindestens acht Zeichen lang sein und mindestens eine Zahl, einen Großbuchstaben, einen Kleinbuchstaben und ein Sonderzeichen (! @ # € % ^ & * - _).

> Nach dem Ändern des Passworts werden Sie automatisch von der GUI abgemeldet und müssen sich mit dem von Ihnen erstellten neuen Passwort erneut anmelden.

**Konfigurieren und Aktivieren der SSO-Funktion**

Mit dieser Anmeldefunktion können Sie XCP-Dateianalysen auf einem bestimmten Computer einrichten und die Web-UI-URL unternehmensweit freigeben, sodass sich Benutzer mit ihren SSO-Anmeldeinformationen (Single Sign-On) bei der Benutzeroberfläche anmelden können.

> Die SSO-Anmeldung ist optional und kann dauerhaft konfiguriert und aktiviert werden. Informationen zum Einrichten von SSO-basierten SSO-Anmeldedaten für die Security Assertion Markup Language (SAML) finden Sie unter Konfigurieren Sie SSO-Anmeldedaten.

3. Nach der Anmeldung sehen Sie den NFS-Agent; ein grünes Häkchen zeigt die minimale Systemkonfiguration des Linux-Systems und der XCP-Version an.
4. Wenn Sie einen SMB-Agent konfiguriert haben, wird der SMB-Agent, der in derselben Agent-Karte hinzugefügt wurde, angezeigt.

### Konfigurieren Sie SSO-Anmeldedaten

Die SSO-Anmeldefunktion wird in XCP File Analytics mithilfe von SAML implementiert und wird vom Active Directory Federation Services (ADFS) Identity Provider unterstützt. SAML verlagert die Authentifizierungsaufgabe an den Drittanbieter-Identitäts-Provider (IdP) für Ihr Unternehmen, der eine Vielzahl von Ansätzen für MFA (Multi-Faktor-Authentifizierung) nutzen kann.

#### Schritte

1. Registrieren Sie die XCP-Dateianalyse-Anwendung beim Identitätsanbieter Ihres Unternehmens.

   Dateianalysen wird jetzt als Service-Provider ausgeführt und muss daher bei Ihrem Identitätsanbieter registriert werden. Im Allgemeinen gibt es im Unternehmen ein Team, das für diesen SSO-Integrationsprozess zuständig ist. Im ersten Schritt können Sie sich an das entsprechende Team wenden und die Metadaten der Dateianalyse-Anwendung mit ihnen teilen.

   Im Folgenden sind die obligatorischen Angaben aufgeführt, die Sie für die Registrierung bei Ihrem Identitätsanbieter freigeben müssen:

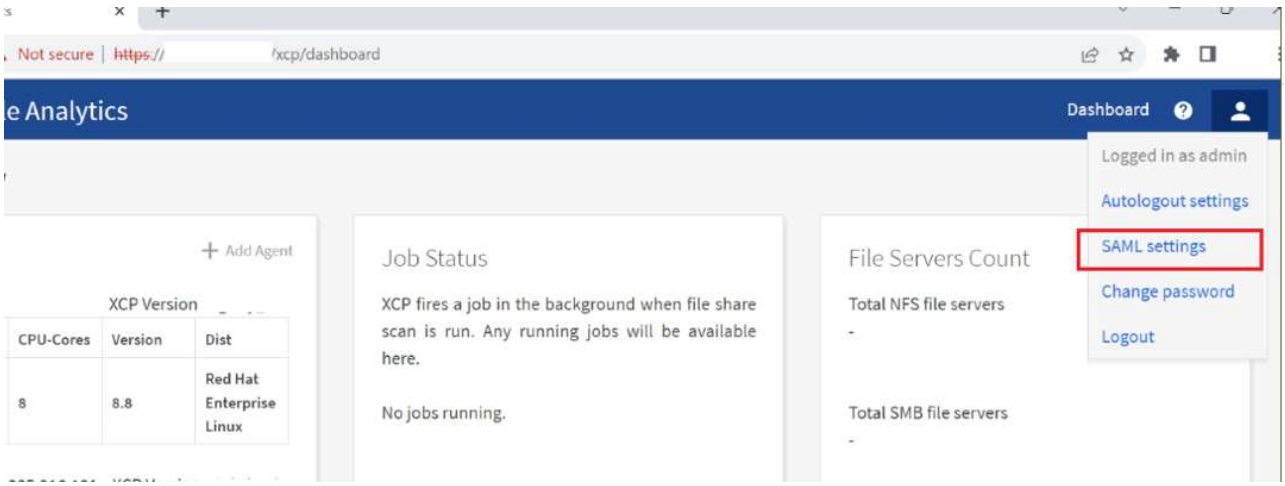
   - **Dienstanbieter Entity ID:** `https://<IP address of linux machine>/xcp`
   - **Service Provider Assertion Consumer Service (ACS) URL:** `https://<IP address of linux machine>:5030/api/xcp/SAML/sp`

     Sie können diese Details auch überprüfen, indem Sie sich in der Benutzeroberfläche für Dateianalysen anmelden:

     i. Melden Sie sich mithilfe der unter beschriebenen Schritte bei der GUI an Melden Sie sich bei der GUI von File Analytics an.

     ii. Wählen Sie oben rechts auf der Seite das Symbol **Benutzer** und dann **SAML-Einstellungen** aus.

     Wählen Sie im angezeigten Dropdown-Menü die Option **Service Provider-Einstellungen** aus.



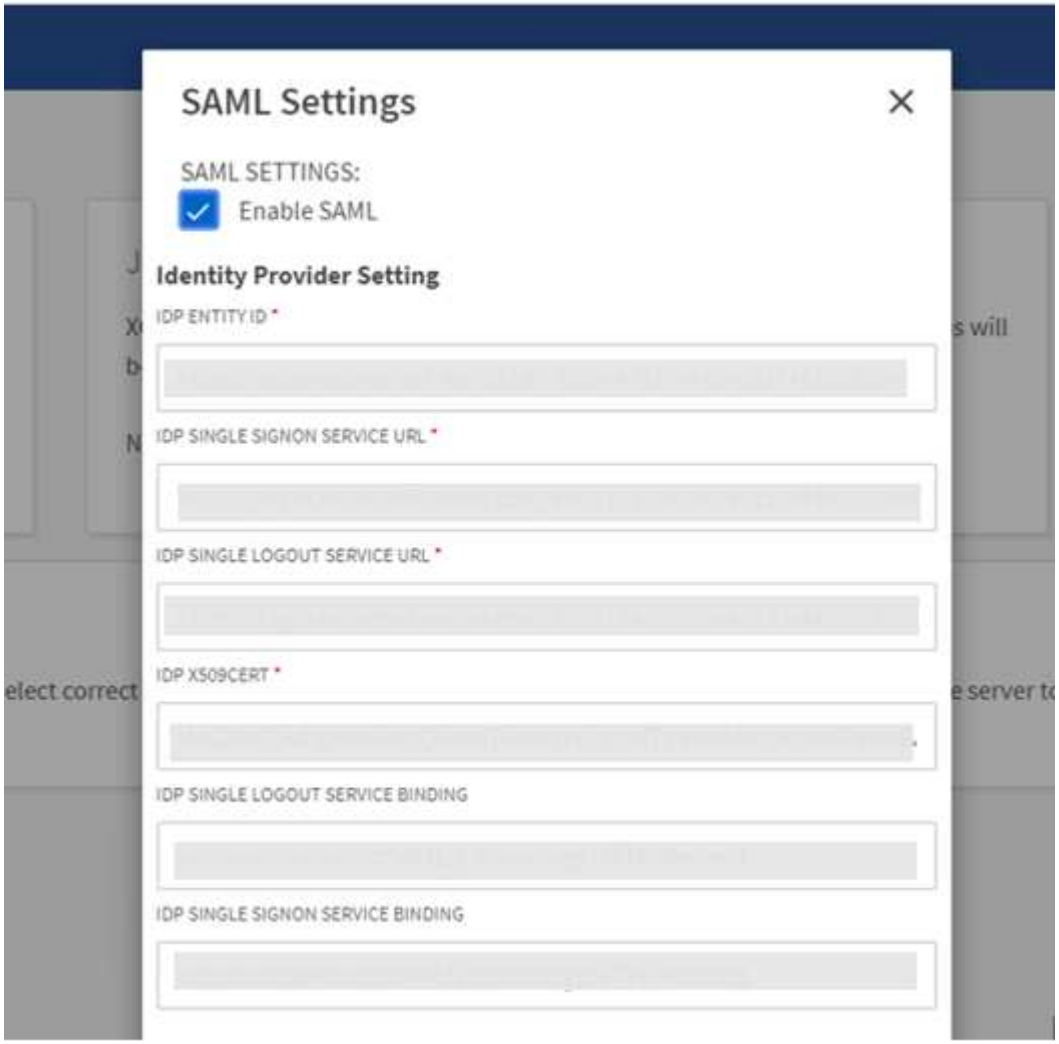

   Nach der Registrierung erhalten Sie die IdP-Endpunktangaben für Ihr Unternehmen. Sie müssen die Metadaten des IdP-Endpunktes für die Dateianalyse-UI bereitstellen.

2. Geben Sie die IdP-Details an:

   a. Gehen Sie zu **Dashboard**. Wählen Sie oben rechts auf der Seite das Symbol **Benutzer** aus und wählen Sie **SAML-Einstellungen**.

b. Geben Sie die IdP-Details ein, die Sie nach der Registrierung erhalten haben.

**Beispiel**




a. Aktivieren Sie das Kontrollkästchen **SAML** aktivieren, um SAML-basiertes SSO dauerhaft zu aktivieren.

b. Wählen Sie **Speichern**.

c. Melden Sie sich von der Dateianalyse ab, und melden Sie sich erneut an.

   Sie werden zur SSO-Seite Ihres Unternehmens umgeleitet.

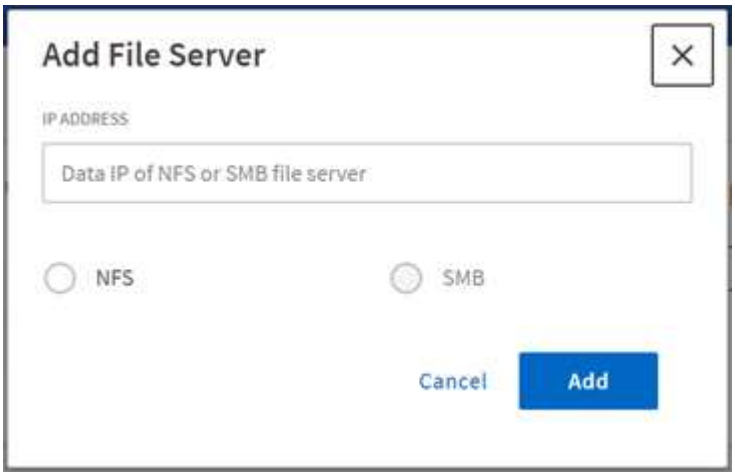
## Fügen Sie Dateiserver hinzu

Sie können in der XCP Dateianalyse-GUI NFS- und SMB-exportierte Dateisysteme konfigurieren.

So kann die XCP-Dateianalyse Daten im Dateisystem scannen und analysieren. Gehen Sie wie folgt vor, um NFS- oder SMB-Dateiserver hinzuzufügen.

**Schritt**

1. Um Dateiserver hinzuzufügen, wählen Sie **Add File Server**.




Fügen Sie die IP-Adresse des Dateiservers hinzu, wählen Sie die NFS- oder SMB-Option aus und klicken Sie auf **Hinzufügen**.

> Wenn ein SMB-Agent in der GUI nicht angezeigt wird, können Sie keinen SMB-Server hinzufügen.

Nach dem Hinzufügen des Dateiservers wird XCP angezeigt:

- Insgesamt verfügbare Dateifreigaben
- Dateifreigaben mit Analysedaten (die anfängliche Anzahl ist „0“, diese wird aktualisiert, wenn Sie einen erfolgreichen Scan ausführen)
- Gesamte Speicherplatzauslastung: Die Summe des von allen Exporten belegten Speicherplatzes
- Die Daten für Dateifreigaben und die Speicherplatzauslastung sind Echtzeitdaten direkt vom NFS/SMB-Server. Das Erfassen und Verarbeiten der Daten dauert mehrere Sekunden.

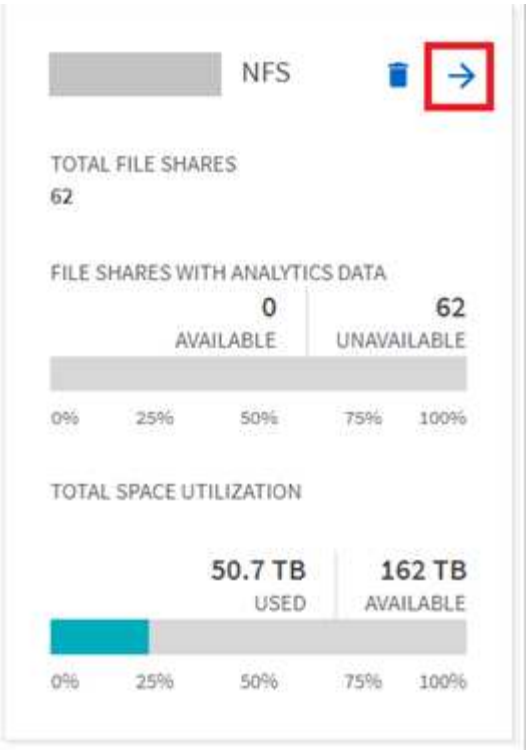
> Der in der Dateianalyse verwendete Speicherplatz im Vergleich zum verfügbaren Speicherplatz wird aus jedem über NFS verfügbaren exportierten File-System berechnet. Wenn beispielsweise die Volumes aus qtrees bestehen und die Exporte über einen qtree erstellt werden, ist der Gesamtspeicherplatz der kumulative Speicherplatz der Volume-Größe und der qtree-Größe.

## Führen Sie einen Scan aus

Wenn das NFS/SMB-Dateisystem zur XCP-Dateianalyse-GUI hinzugefügt wird, können Sie einen Dateisystemscan starten, um die Daten zu analysieren und darzustellen.

### Schritte

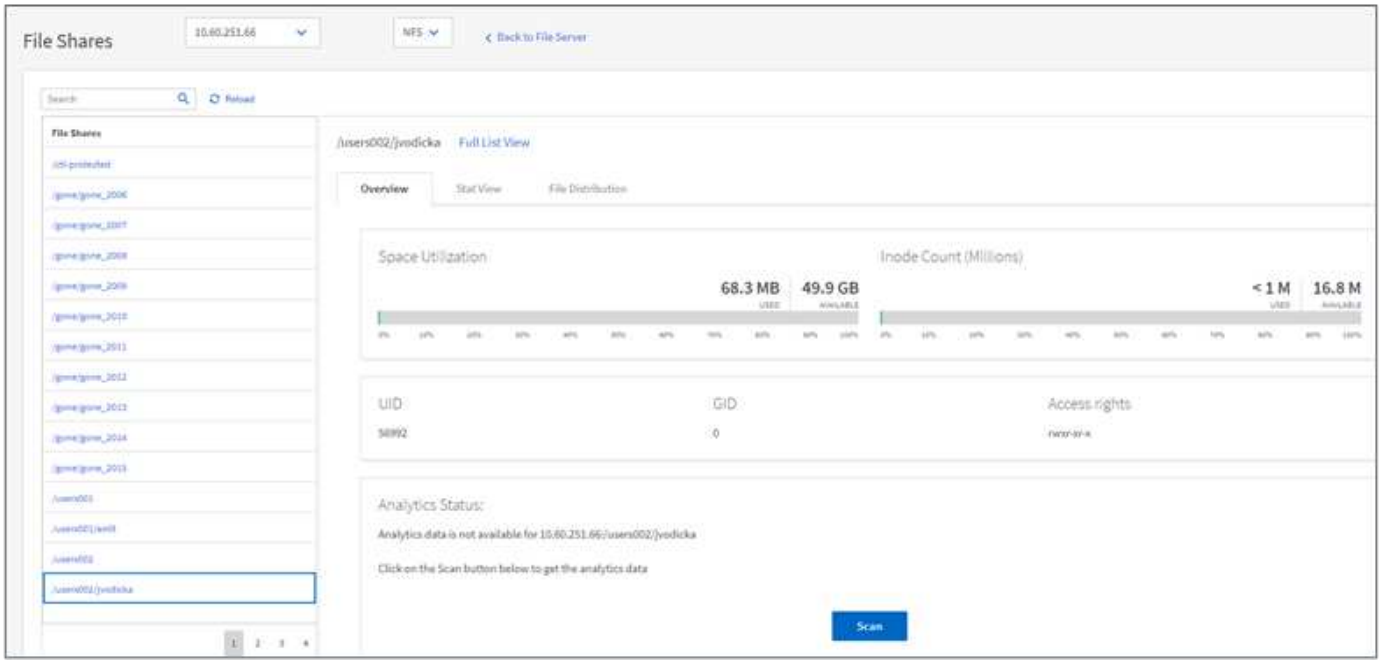
1. Wählen Sie den Pfeil auf der hinzugefügten Dateiserverkarte aus, um die Dateifreigaben auf dem Dateiserver anzuzeigen.




2. Wählen Sie aus der Liste der Dateifreigaben den Namen der zu scannenden Dateifreigabe aus.
3. Wählen Sie **Scannen**, um den Scan zu starten.

   XCP zeigt eine Statusleiste für den Scan an.

4. Wenn der Scan abgeschlossen ist, sind die Registerkarten **stat view** und **file Distribution** aktiviert, damit Sie Diagramme anzeigen können.



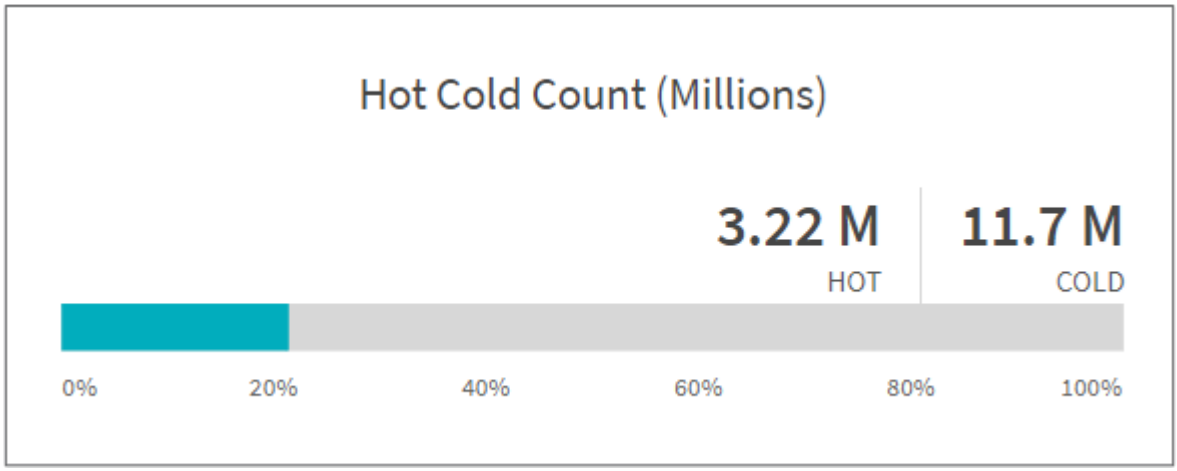

### Erfahren Sie mehr über Diagramme

Über das GUI-Dashboard von Dateianalysen werden mehrere Diagramme zur Visualisierung von

Dateianalysen angezeigt.

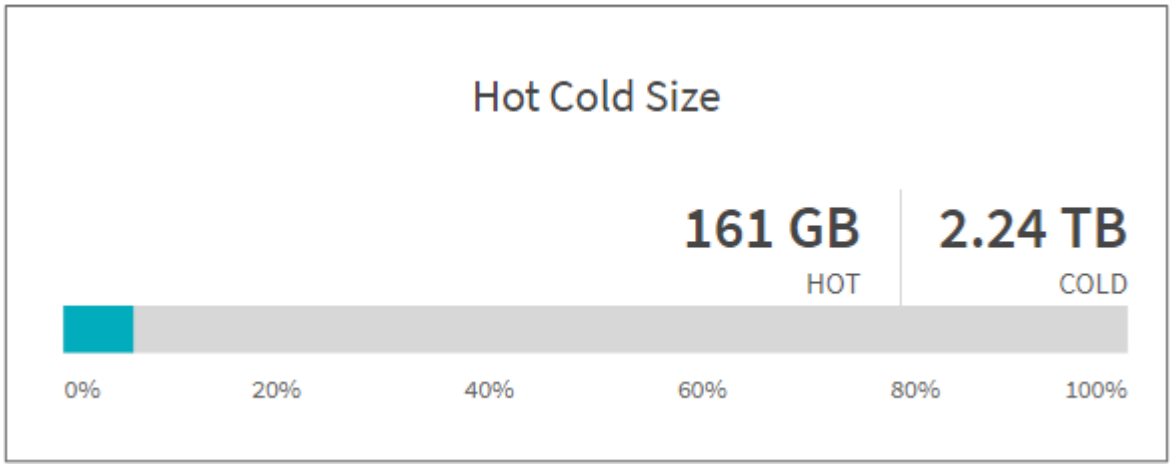
#### Diagramm „Heiße Kalte Daten“

XCP File Analytics kategorisiert Dateien, auf die 90 Tage lang nicht zugegriffen wird, als kalte Daten. Dateien, auf die in den letzten 90 Tagen zugegriffen wird, sind wichtige Daten. Die Definition wichtiger und „kalter“ Daten basiert ausschließlich auf der Zugriffszeit.




Im Diagramm „Hot Cold Count“ wird die Anzahl der Inodes (in Millionen) angezeigt, die im XCP NFS heiß oder kalt sind. In XCP SMB gibt dieses Diagramm die Anzahl der Dateien an, die heiß oder kalt sind. Der farbige Balken stellt die heißen Daten dar und zeigt den Prozentsatz der Dateien an, auf die innerhalb von 90 Tagen zugegriffen wird.

#### Diagramm „Heiße Kalte“ Größe




Das Diagramm „heiße kalte Größe“ zeigt den Prozentsatz der Dateien an, die heiß und kalt sind, und die Gesamtgröße der Dateien in jeder Kategorie. Der farbige Balken stellt die heißen Daten dar und der unfarbige Teil stellt die kalten Daten dar. Die Definition wichtiger und „kalter“ Daten basiert ausschließlich auf der Zugriffszeit.

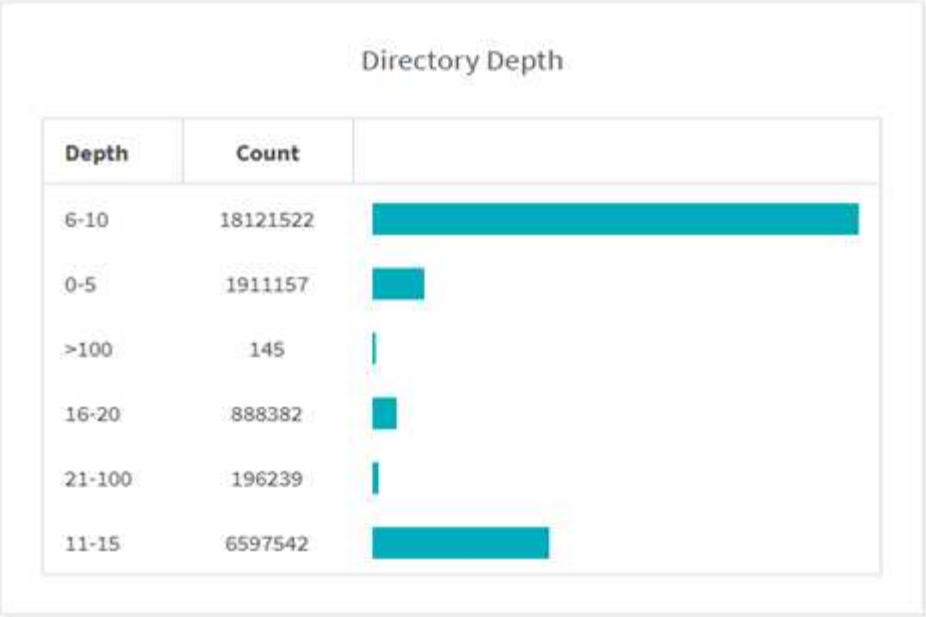
#### Einträge im Verzeichnisdiagramm

Die Einträge im Diagramm Verzeichnisse zeigen die Anzahl der Einträge in Verzeichnissen an. Die Spalte Tiefe enthält unterschiedliche Verzeichnisgrößen und die Spalte Anzahl gibt die Anzahl der Einträge in jeder Verzeichnistiefe an.

**Dateiverteilung nach Größendiagramm**

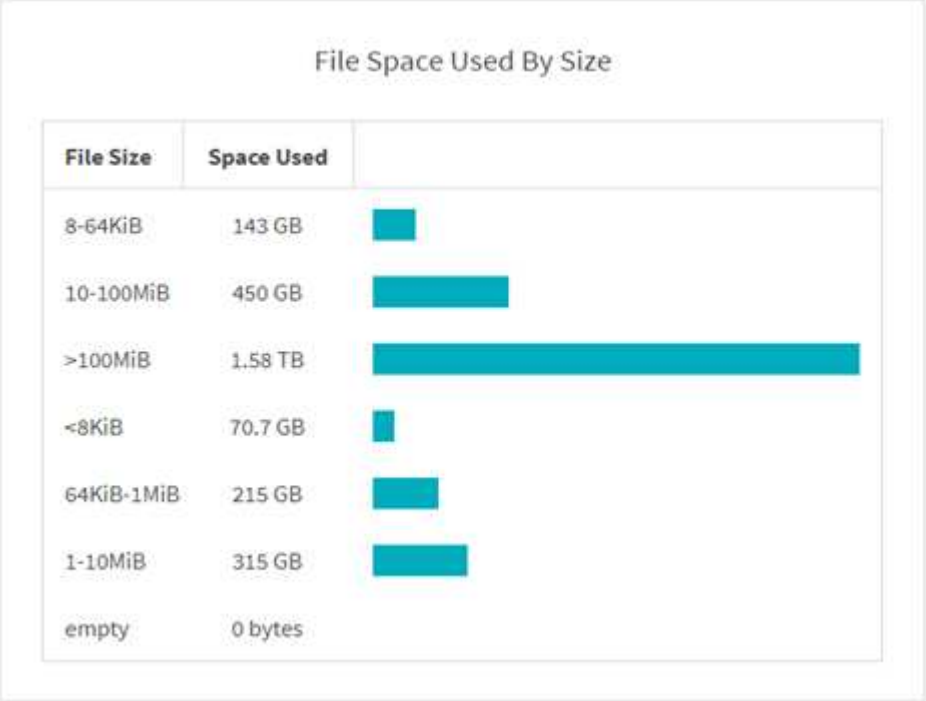
Im Diagramm Dateiverteilung nach Größe wird die Anzahl der Dateien angezeigt, die unter den angegebenen Dateigrößen liegen. Die Spalte Dateigröße enthält die Kategorien der Dateigröße und die Spalte Anzahl gibt die Verteilung der Anzahl der Dateien an.

**Diagramm Für Die Verzeichnistiefe**



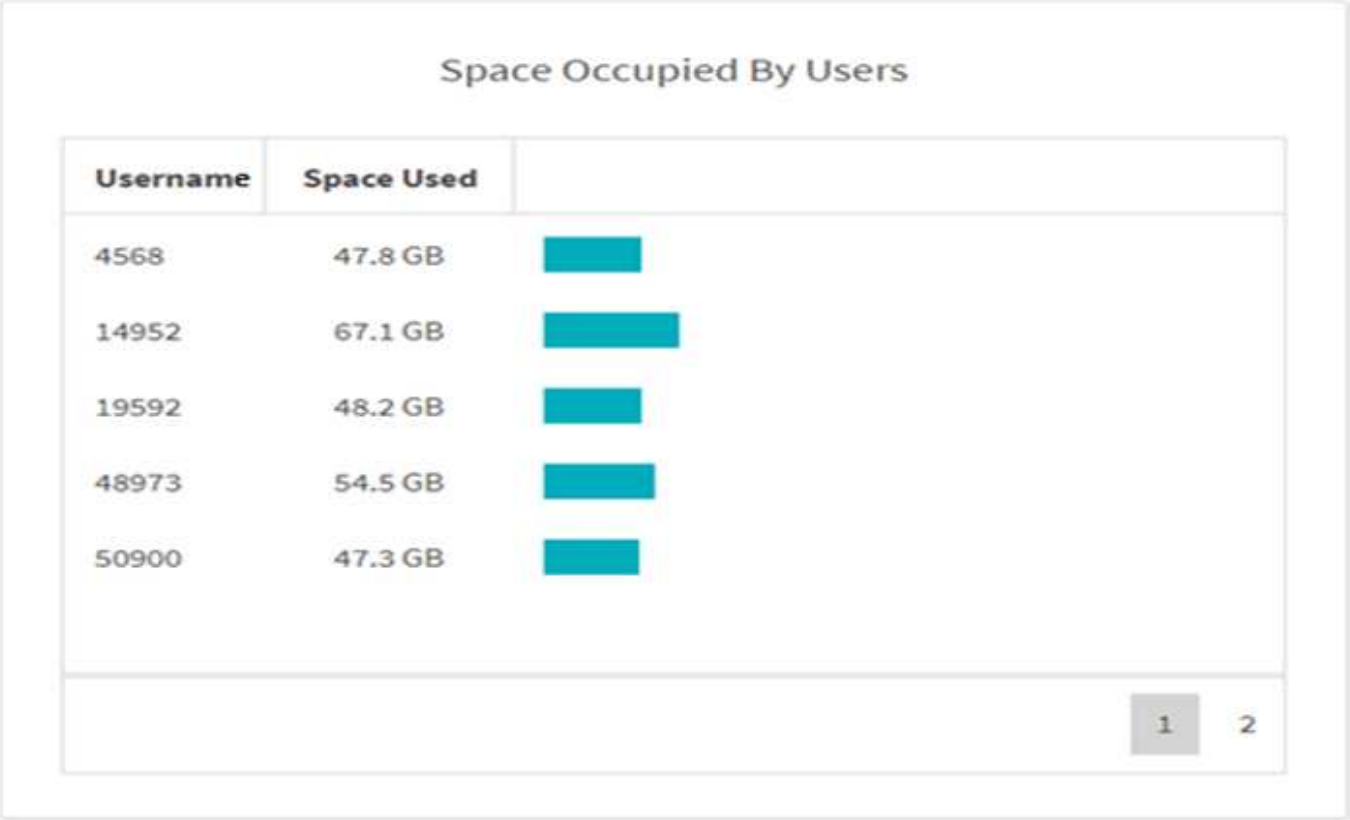

Das Diagramm Verzeichnistiefe stellt die Verteilung der Anzahl der Verzeichnisse in verschiedenen Verzeichnis-Tiefenbereichen dar. Die Spalte Tiefe enthält verschiedene Verzeichnistiefen, und die Spalte Anzahl enthält die Anzahl der einzelnen Verzeichnistiefen in der Dateifreigabe.

**Nach Größendiagramm verwendeter Dateiraum**



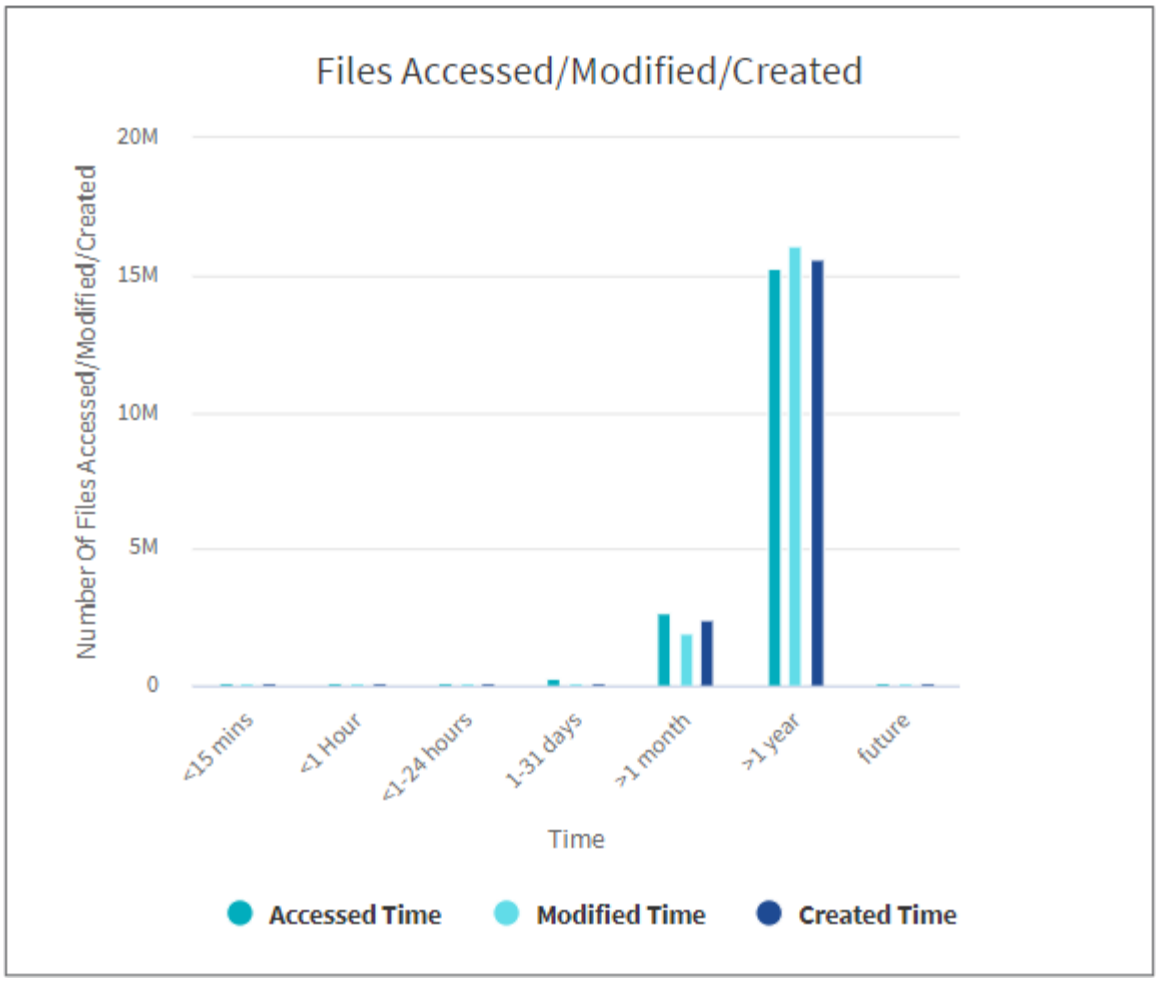

Im Diagramm „Dateibereich“ wird die Anzahl der Dateien in unterschiedlichen Dateigrößen angezeigt. Die Spalte Dateigröße enthält unterschiedliche Dateigrößen, und in der Spalte „verwendeter Speicherplatz“ wird der Speicherplatz angegeben, der von jedem Dateigrößenbereich verwendet wird.

**Speicherplatz belegt durch Benutzer Diagramm**




Das Diagramm „von Benutzern belegter Speicherplatz“ zeigt den von Benutzern verwendeten Speicherplatz an. Die Spalte Benutzername enthält die Namen von Benutzern (UID, wenn Benutzernamen nicht abgerufen werden können) und die Spalte „verwendeter Raum“ gibt den von jedem Benutzernamen verwendeten Platz an.

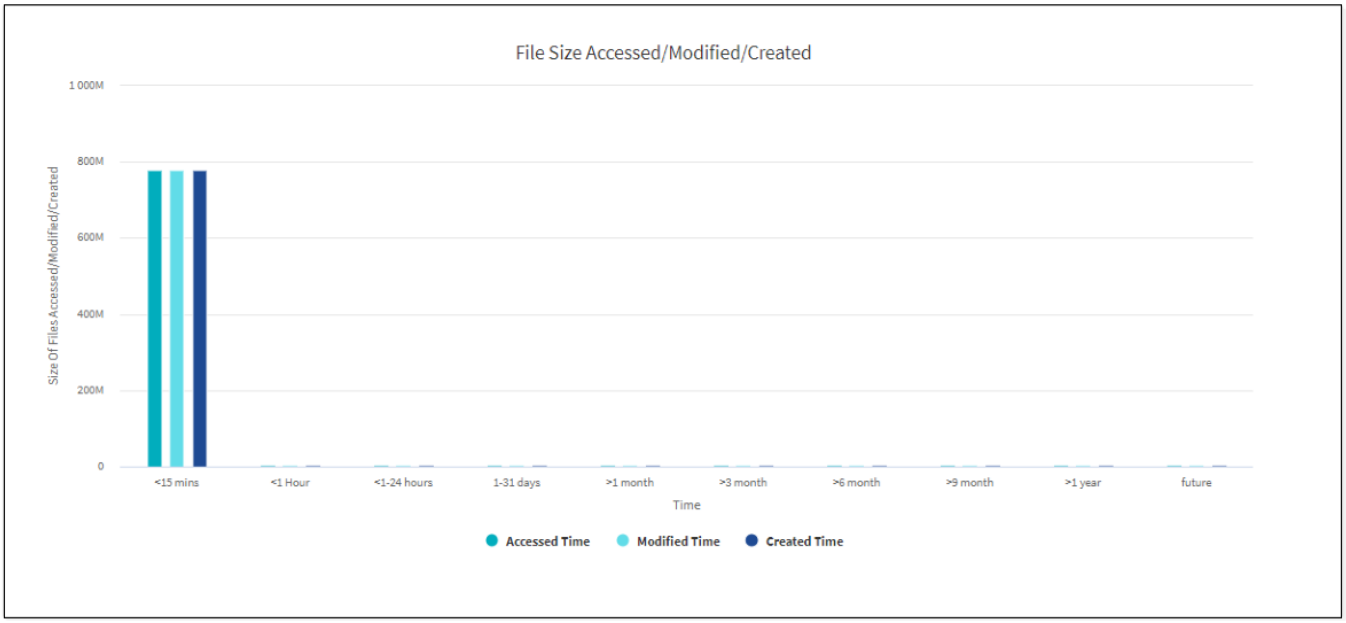
**Dateien, Auf Die Zugegriffen Wurde/Geändert/Erstellt Wurde**




Im Diagramm Dateien abgerufen/geändert/erstellt wird die Anzahl der im Laufe der Zeit geänderten Dateien angezeigt. Die X-Achse repräsentiert den Zeitraum, in dem Änderungen vorgenommen wurden, und die Y-Achse repräsentiert die Anzahl der geänderten Dateien.

> Um das Diagramm für die Zugriffszeit (Atime) in SMB-Scans anzuzeigen, aktivieren Sie das Kontrollkästchen, um vor dem Ausführen eines Scans eine Zeitdauer zu erhalten.

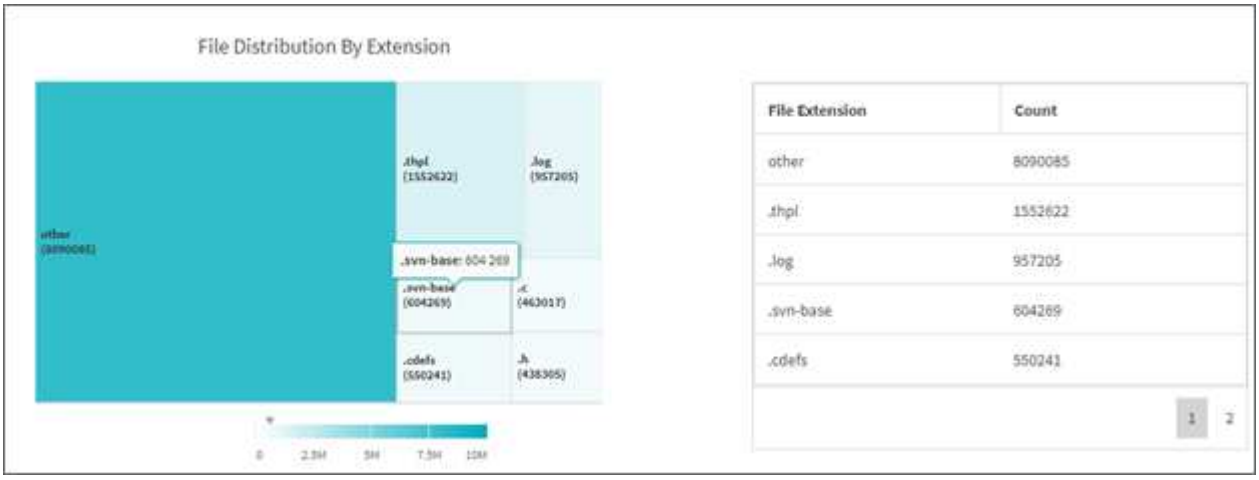
**Diagramm „Dateigröße Zugegriffen/Geändert/Erstellt“**




Das Diagramm „Dateigröße zugegriffen/geändert/erstellt“ zeigt die Größe der Dateien an, die im Laufe der Zeit geändert wurden. Die X-Achse repräsentiert den Zeitraum, innerhalb dessen Änderungen vorgenommen wurden, und die Y-Achse repräsentiert die Größe der geänderten Dateien.

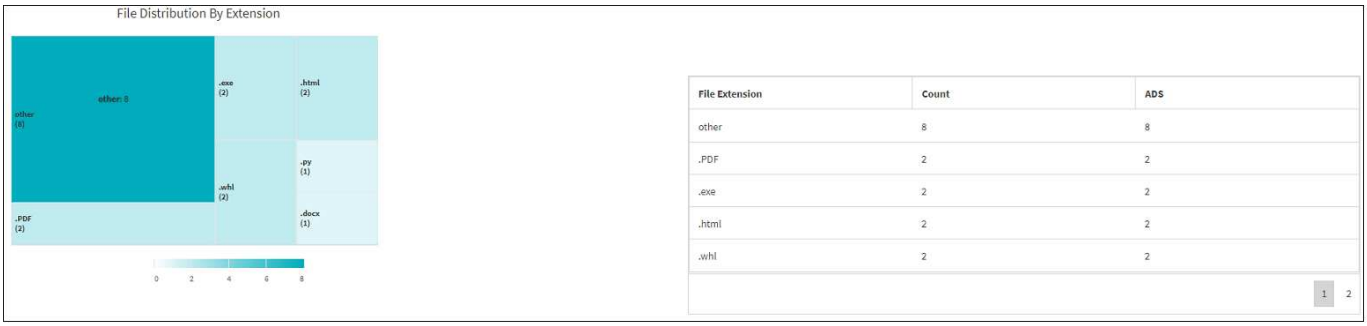
> Um das Diagramm für die Zugriffszeit (Atime) in SMB-Scans anzuzeigen, aktivieren Sie das Kontrollkästchen, um vor dem Ausführen eines Scans eine Zeitdauer zu erhalten.

**Dateiverteilung nach Erweiterung Graph**




Das Diagramm Dateiverteilung nach Erweiterung stellt die Anzahl der verschiedenen Dateierweiterungen in einer Dateifreigabe dar. Die Größe der Divisionen, die die Erweiterungen darstellen, basiert auf der Anzahl der Dateien mit jeder Erweiterung.

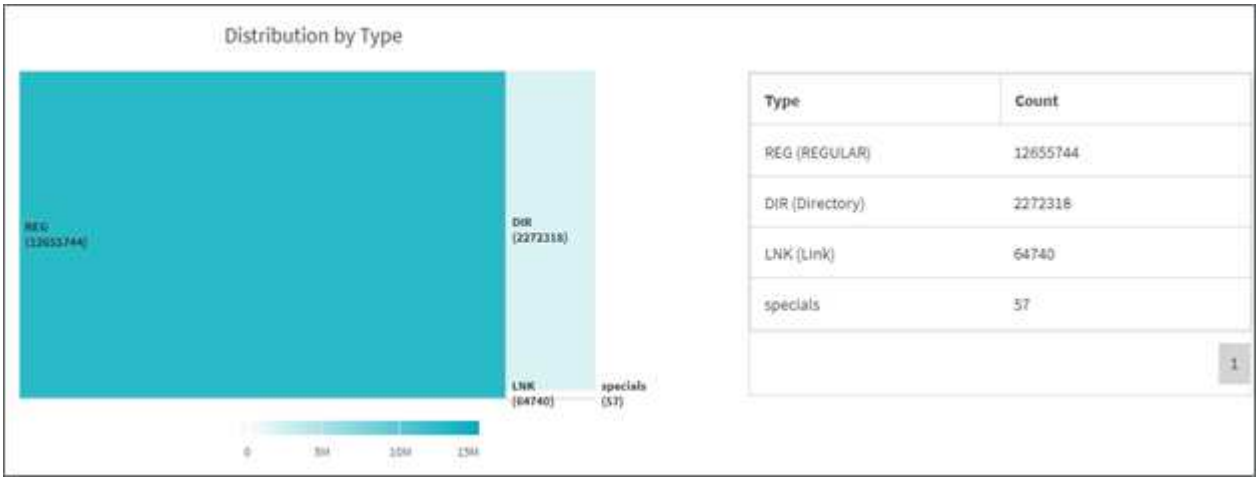
Darüber hinaus können Sie bei SMB-Freigaben die Anzahl der alternativen Datenströme (ADS)-Dateien für jede Dateierweiterung abrufen, indem Sie das Kontrollkästchen für ADS aktivieren, bevor Sie einen Scan ausführen.




**Dateigrößenverteilung nach Erweiterung Graph**

Das Diagramm Dateigrößenverteilung nach Erweiterung stellt die kumulative Größe der verschiedenen Dateierweiterungen in einer Dateifreigabe dar. Die Größe der Divisionen, die die Erweiterungen darstellen, basiert auf der Größe der Dateien mit jeder Erweiterung.

**Dateiverteilung nach Typ Diagramm**




Das Diagramm Verteilung nach Typ stellt die Anzahl der folgenden Dateitypen dar:

- REG: Normale Dateien
- LNK: Dateien mit Links
- Specials: Dateien mit Gerätedateien und Zeichendateien.
- DIR: Dateien mit Verzeichnissen

- Verbindung: Nur in SMB verfügbar

Darüber hinaus können Sie bei SMB-Freigaben die Anzahl der alternativen Datenströme (ADS)-Dateien für verschiedene Typen abrufen, indem Sie das Kontrollkästchen für ANZEIGEN aktivieren, bevor Sie einen Scan ausführen.

# Filter

## XCP bietet Filteroptionen, die für XCP-Vorgänge verwendet werden können.

XCP verwendet Filter für `-match` Und `-exclude` Optionen für NFS und SMB:

Für NFS: Führen Sie aus `xcp help info` Und im Abschnitt FILTER erfahren Sie, wie Sie diese verwenden `-match` Und `-exclude` Filter.

Für SMB: Führen Sie aus `xcp help -match` Und `xcp help -exclude` Um weitere Informationen zu erhalten `match` Und `exclude` Filter.

Wenn Sie Filter in XCP-Befehlen verwenden möchten, führen Sie aus `xcp help <command>` Um festzustellen, ob es sich um unterstützte Optionen handelt.

# Protokollierung für NFS und SMB (optional)

## Protokollierung für XCP NFS und SMB.

XCP unterstützt die Konfiguration mehrerer optionaler Funktionen mit dem `xcpLogConfig.json` JSON-Konfigurationsdatei Um nur bestimmte Funktionen zu aktivieren, erstellen Sie manuell das `xcpLogConfig.json` Konfigurationsdatei Sie können das verwenden `xcpLogConfig.json` Konfigurationsdatei zum Aktivieren:

- Ereignisprotokollmeldungen
- Syslog-Client für XCP
- Benutzerdefinierte XCP-Protokollierung

In der Standardkonfiguration sind Ereignisprotokollmeldungen und der syslog-Client deaktiviert. Die Konfiguration ist für NFS und SMB üblich.

| JSON-Dateispeicherort konfigurieren | NFS | SMB |
|---|---|---|
| Standardspeicherort der Konfigurationsdatei | /Opt/NetApp/Xfiles/xcp/ | C:\NetApp\XCP\ConfigFile |
| Benutzerdefinierter Standort erfordert den `XCP_CONFIG_DIR` Umgebungsvariable | Verwenden Sie die Position, die Sie gegen den festgelegt haben `XCP_CONFIG_DIR` Variabel | K. A. |

Bei den Optionen der JSON-Konfigurationsdatei wird zwischen Groß- und Kleinschreibung unterschieden. Diese Optionen sind für XCP NFS und XCP SMB identisch.

| Name der Unteroptionen | JSON-Datentyp | Standard | Beschreibung |
|---|---|---|---|
| Logkonfig | | | Option zum Anpassen der XCP-Protokollierung. |
| „Ebene“ | Zeichenfolge | INFO | Filterstufe für Protokollmeldung, Schweregrad XCP-Protokollmeldungen unterstützen fünf Schweregrade in Reihenfolge des Schweregrads für die Verringerung des Schweregrads: KRITISCH, FEHLER, WARNUNG, INFO, DEBUG (NetApp empfiehlt dringend INFORMATIONEN oder DEBUG) |
| „MaxBytes“ | Ganzzahl | 52428800 | Größe jeder rotierenden Protokolldatei. Maximal unterstützte Rotationsdateien sind 10. |
| „Name“ | Zeichenfolge | xcp.log | Option zum Festlegen des benutzerdefinierten Protokolldateinamens. |
| Eventlog | | | Option zum Konfigurieren der Ereignisprotokollmeldung. |
| „Isenabled“ | Boolesch | Richtig | Diese boolesche Option wird zum Aktivieren der Ereignisnachrichten verwendet. Einstellen auf `false` Werden keine Ereignismeldungen generiert, und es werden keine Ereignisprotokolle in der Ereignis-Log-Datei veröffentlicht. |
| „Ebene“ | Zeichenfolge | INFO | Filterebene für Ereignismeldung: Schweregrad Event Messaging unterstützt fünf Schweregrade in der Reihenfolge des abnehmenden Schweregrads: KRITISCH, FEHLER, WARNUNG, INFO, DEBUG |
| Syslog | | | Option zum Konfigurieren von Syslog-Messaging. |
| „Isenabled“ | Boolesch | Falsch | Diese boolesche Option wird verwendet, um Syslog-Client in XCP zu aktivieren. |
| „Ebene“ | Zeichenfolge | INFO | Filterstufe für Meldungen mit Schweregrad. XCP-Ereignisprotokollmeldungen unterstützen fünf Schweregrade in der Reihenfolge des Schweregrads: KRITISCH, FEHLER, WARNUNG, INFO, DEBUG |
| „ServerIP“ | Zeichenfolge | Keine | IP-Adressen oder Hostname des Remote-Syslog-Servers. |

| Name der Unteroptionen | JSON-Datentyp | Standard | Beschreibung |
|---|---|---|---|
| „Port“ | Ganzzahl | 514 | Remote-Syslog-Empfänger-Port. Syslog-Empfänger, die Syslog-Datagramme auf einem anderen Port akzeptieren, können mit der Port-Option UDP-Port 514 konfiguriert werden, Sie können aber auch an den gewünschten Port konfigurieren. |
| „Desinfizieren“ | Boolesch | Falsch | Eine allgemeine Option für XCP-Unterstützung; wenn ihr Wert auf „true“ gesetzt wird, werden vertrauliche Informationen (IP und Benutzername) in den zu unterstützenden Meldungen (Protokollierung, Ereignisse, Syslog usw.) verborgen. Zum Beispiel mit `sanitize` Option als `false`: * `2020-07-17 03:10:23,779 - INFO - 12806 xcp xcp Paths: ['10.234.104.251:/cat_vol']* 2020-07-17 03:10:23,778 - INFO - 12806 xcp xcp User Name: root`Mit dem `sanitize` Option als `true`: * `2020-07-17 03:13:51,596 - INFO - 12859 xcp xcp Paths: ['IP: XX.XX.XX.XX:/cat_vol']* 2020-07-17 03:13:51,595 - INFO - 12859 xcp xcp User Name: * * *` |

## Erstellen Sie die JSON-Konfigurationsdatei

Wenn Sie Ereignisprotokollmeldungen, den Syslog-Client oder die Kundenprotokollierung aktivieren möchten, führen Sie die folgenden Schritte aus.

**Schritte**

1. Öffnen Sie einen beliebigen Texteditor, z. B. Editor oder vi.
2. Erstellen Sie eine neue Datei mit der folgenden JSON-Vorlage.

```
{
  "logConfig": {
    "level": "INFO",
    "maxBytes": 52428800,
    "name": "xcp.log"
  },
  "eventlog": {
    "isEnabled": false,
    "level": "INFO"
  },
  "syslog": {
    "isEnabled": false,
    "level": "INFO",
    "serverIp": "10.234.219.87",
    "port": 514
  },
  "sanitize": false
}
```

3. Ändern Sie für alle Funktionen, die Sie aktivieren möchten `isEnabled` Mehrwert für `true`.
4. Benennen Sie die Datei `xcpLogConfig.json` Und speichern Sie sie am Standardspeicherort: /Opt/NetApp/Xfiles/xcp/

   Wenn der `XCP_CONFIG_DIR` Umgebungsvariable ist festgelegt, speichern Sie die `xcpLogConfig.json` Datei an demselben Speicherort, der für das festgelegt ist `XCP_CONFIG_DIR` Variabel.

| Standardkonfiguration | Beispiel für eine Json-Konfigurationsdatei |
| --- | --- |
| `{ "logConfig": { "level": "INFO", "maxBytes": 52428800, "name": "xcp.log" }, "sanitize": false }` | `{ "logConfig": { "level": "INFO", "maxBytes": 52428800, "name": "xcp.log" }, "eventlog": { "isEnabled": false, "level": "INFO" }, "syslog": { "isEnabled": false, "level": "INFO", "serverIp": "10.234.219.87", "port": 514 }, "sanitize": false }` |

**Copyright-Informationen**

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtsinhabers in keiner Form und durch keine Mittel – weder grafische noch elektronische oder mechanische, einschließlich Fotokopieren, Aufnehmen oder Speichern in einem elektronischen Abrufsystem – auch nicht in Teilen, vervielfältigt werden.

Software, die von urheberrechtlich geschütztem NetApp Material abgeleitet wird, unterliegt der folgenden Lizenz und dem folgenden Haftungsausschluss:

DIE VORLIEGENDE SOFTWARE WIRD IN DER VORLIEGENDEN FORM VON NETAPP ZUR VERFÜGUNG GESTELLT, D. H. OHNE JEGLICHE EXPLIZITE ODER IMPLIZITE GEWÄHRLEISTUNG, EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE STILLSCHWEIGENDE GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT UND EIGNUNG FÜR EINEN BESTIMMTEN ZWECK, DIE HIERMIT AUSGESCHLOSSEN WERDEN. NETAPP ÜBERNIMMT KEINERLEI HAFTUNG FÜR DIREKTE, INDIREKTE, ZUFÄLLIGE, BESONDERE, BEISPIELHAFTE SCHÄDEN ODER FOLGESCHÄDEN (EINSCHLIESSLICH, JEDOCH NICHT BESCHRÄNKT AUF DIE BESCHAFFUNG VON ERSATZWAREN ODER -DIENSTLEISTUNGEN, NUTZUNGS-, DATEN- ODER GEWINNVERLUSTE ODER UNTERBRECHUNG DES GESCHÄFTSBETRIEBS), UNABHÄNGIG DAVON, WIE SIE VERURSACHT WURDEN UND AUF WELCHER HAFTUNGSTHEORIE SIE BERUHEN, OB AUS VERTRAGLICH FESTGELEGTER HAFTUNG, VERSCHULDENSUNABHÄNGIGER HAFTUNG ODER DELIKTSHAFTUNG (EINSCHLIESSLICH FAHRLÄSSIGKEIT ODER AUF ANDEREM WEGE), DIE IN IRGENDEINER WEISE AUS DER NUTZUNG DIESER SOFTWARE RESULTIEREN, SELBST WENN AUF DIE MÖGLICHKEIT DERARTIGER SCHÄDEN HINGEWIESEN WURDE.

NetApp behält sich das Recht vor, die hierin beschriebenen Produkte jederzeit und ohne Vorankündigung zu ändern. NetApp übernimmt keine Verantwortung oder Haftung, die sich aus der Verwendung der hier beschriebenen Produkte ergibt, es sei denn, NetApp hat dem ausdrücklich in schriftlicher Form zugestimmt. Die Verwendung oder der Erwerb dieses Produkts stellt keine Lizenzierung im Rahmen eines Patentrechts, Markenrechts oder eines anderen Rechts an geistigem Eigentum von NetApp dar.

Das in diesem Dokument beschriebene Produkt kann durch ein oder mehrere US-amerikanische Patente, ausländische Patente oder anhängige Patentanmeldungen geschützt sein.

ERLÄUTERUNG ZU „RESTRICTED RIGHTS“: Nutzung, Vervielfältigung oder Offenlegung durch die US-Regierung unterliegt den Einschränkungen gemäß Unterabschnitt (b)(3) der Klausel „Rights in Technical Data – Noncommercial Items“ in DFARS 252.227-7013 (Februar 2014) und FAR 52.227-19 (Dezember 2007).

Die hierin enthaltenen Daten beziehen sich auf ein kommerzielles Produkt und/oder einen kommerziellen Service (wie in FAR 2.101 definiert) und sind Eigentum von NetApp, Inc. Alle technischen Daten und die Computersoftware von NetApp, die unter diesem Vertrag bereitgestellt werden, sind gewerblicher Natur und wurden ausschließlich unter Verwendung privater Mittel entwickelt. Die US-Regierung besitzt eine nicht ausschließliche, nicht übertragbare, nicht unterlizenzierbare, weltweite, limitierte unwiderrufliche Lizenz zur Nutzung der Daten nur in Verbindung mit und zur Unterstützung des Vertrags der US-Regierung, unter dem die Daten bereitgestellt wurden. Sofern in den vorliegenden Bedingungen nicht anders angegeben, dürfen die Daten ohne vorherige schriftliche Genehmigung von NetApp, Inc. nicht verwendet, offengelegt, vervielfältigt, geändert, aufgeführt oder angezeigt werden. Die Lizenzrechte der US-Regierung für das US-Verteidigungsministerium sind auf die in DFARS-Klausel 252.227-7015(b) (Februar 2014) genannten Rechte beschränkt.

**Markeninformationen**

NETAPP, das NETAPP Logo und die unter http://www.netapp.com/TM aufgeführten Marken sind Marken von NetApp, Inc. Andere Firmen und Produktnamen können Marken der jeweiligen Eigentümer sein.