



Konfigurieren der Single Sign-On-Konfiguration

StorageGRID 11.5

NetApp
April 11, 2024

Inhalt

- Konfigurieren der Single Sign-On-Konfiguration 1
 - Bestätigung der föderierten Benutzer kann sich anmelden 1
 - Sandbox-Modus verwenden 3
 - Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS 5
 - Testen von Vertrauen von Vertrauensstellen 11
 - Aktivieren von Single Sign On 13
 - Deaktivieren der Einzelanmeldung 14
 - Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten 14

Konfigurieren der Single Sign-On-Konfiguration

Wenn Single Sign-On (SSO) aktiviert ist, können Benutzer nur auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API oder die Mandantenmanagement-API zugreifen, wenn ihre Anmeldedaten über den von Ihrem Unternehmen implementierten SSO-Anmeldeprozess autorisiert sind.

- ["Bestätigung der föderierten Benutzer kann sich anmelden"](#)
- ["Sandbox-Modus verwenden"](#)
- ["Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS"](#)
- ["Testen von Vertrauen von Vertrauensstellen"](#)
- ["Aktivieren von Single Sign On"](#)
- ["Deaktivieren der Einzelanmeldung"](#)
- ["Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten"](#)

Bestätigung der föderierten Benutzer kann sich anmelden

Bevor Sie Single Sign-On (SSO) aktivieren, müssen Sie bestätigen, dass sich mindestens ein verbundener Benutzer beim Grid Manager und beim Tenant Manager für alle bestehenden Mandantenkonten anmelden kann.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie verwenden Active Directory als föderierte Identitätsquelle und AD FS als Identitätsanbieter.

["Anforderungen für die Nutzung von Single Sign On"](#)

Schritte

1. Falls bereits vorhandene Mandantenkonten vorhanden sind, bestätigen Sie, dass kein Mandant seine eigene Identitätsquelle verwendet.



Wenn Sie SSO aktivieren, wird eine im Mandantenmanager konfigurierte Identitätsquelle von der im Grid Manager konfigurierten Identitätsquelle außer Kraft gesetzt. Benutzer, die zur Identitätsquelle des Mandanten gehören, können sich nicht mehr anmelden, es sei denn, sie verfügen über ein Konto bei der Identitätsquelle des Grid Manager.

- a. Melden Sie sich für jedes Mandantenkonto bei Tenant Manager an.
 - b. Wählen Sie **Zugriffskontrolle > Identitätsföderation**.
 - c. Bestätigen Sie, dass das Kontrollkästchen **Identitätsföderation aktivieren** nicht aktiviert ist.
 - d. Wenn dies der Fall ist, bestätigen Sie, dass alle föderierten Gruppen, die für dieses Mandantenkonto verwendet werden, nicht mehr erforderlich sind. Deaktivieren Sie das Kontrollkästchen, und klicken Sie auf **Speichern**.
2. Bestätigen Sie, dass ein verbundener Benutzer auf den Grid Manager zugreifen kann:

- a. Wählen Sie im Grid Manager die Option **Konfiguration > Zugriffskontrolle > Admin-Gruppen** aus.
 - b. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus der Active Directory-Identitätsquelle importiert wurde und dass ihr die Root-Zugriffsberechtigung zugewiesen wurde.
 - c. Abmelden.
 - d. Bestätigen Sie, dass Sie sich wieder bei Grid Manager als Benutzer in der föderierten Gruppe anmelden können.
3. Wenn es bereits vorhandene Mandantenkonten gibt, bestätigen Sie, dass sich ein föderaler Benutzer mit Root Access-Berechtigung anmelden kann:
- a. Wählen Sie im Grid Manager die Option **Miters** aus.
 - b. Wählen Sie das Mandantenkonto aus und klicken Sie auf **Konto bearbeiten**.
 - c. Wenn das Kontrollkästchen *** verwendet eigene Identitätsquelle*** aktiviert ist, deaktivieren Sie das Kontrollkästchen und klicken Sie auf **Speichern**.

Edit Tenant Account

Tenant Details

Display Name

Uses Own Identity Source

Allow Platform Services

Storage Quota (optional) GB ▼

Cancel
Save

Die Seite Mandantenkonten wird angezeigt.

- a. Wählen Sie das Mandantenkonto aus, klicken Sie auf **Anmelden** und melden Sie sich als lokaler Root-Benutzer beim Mandantenkonto an.
- b. Klicken Sie im Mandantenmanager auf **Zugriffskontrolle > Gruppen**.
- c. Stellen Sie sicher, dass mindestens eine föderierte Gruppe aus dem Grid Manager der Root Access-Berechtigung für diesen Mandanten zugewiesen wurde.
- d. Abmelden.
- e. Bestätigen Sie, dass Sie sich wieder bei dem Mandanten als Benutzer in der föderierten Gruppe anmelden können.

Verwandte Informationen

["Anforderungen für die Nutzung von Single Sign On"](#)

["Verwalten von Admin-Gruppen"](#)

["Verwenden Sie ein Mandantenkonto"](#)

Sandbox-Modus verwenden

Sie können den Sandbox-Modus verwenden, um Active Directory Federation Services (AD FS) zu konfigurieren und zu testen, die auf Vertrauen von Parteien basieren, bevor Sie SSO für StorageGRID-Benutzer durchsetzen. Nachdem SSO aktiviert ist, können Sie den Sandbox-Modus erneut aktivieren, um neue und vorhandene Vertrauensstellen zu konfigurieren oder zu testen. Im Sandbox-Modus wird SSO für StorageGRID-Benutzer vorübergehend deaktiviert.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

Über diese Aufgabe

Wenn SSO aktiviert ist und ein Benutzer versucht, sich bei einem Admin-Node anzumelden, sendet StorageGRID eine Authentifizierungsanforderung an AD FS. Wiederum sendet AD FS eine Authentifizierungsantwort zurück an StorageGRID, die angibt, ob die Autorisierungsanforderung erfolgreich war. Für erfolgreiche Anforderungen enthält die Antwort eine universell eindeutige Kennung (UUID) für den Benutzer.

Damit StorageGRID (der Service Provider) und AD FS (der Identitäts-Provider) sicher über Benutzerauthentifizierungsanforderungen kommunizieren können, müssen Sie bestimmte Einstellungen in StorageGRID konfigurieren. Als Nächstes müssen Sie AD FS verwenden, um für jeden Admin-Knoten ein Vertrauensverhältnis zu erstellen. Abschließend müssen Sie zu StorageGRID zurückkehren, um SSO zu aktivieren.

Im Sandbox-Modus ist es einfach, diese Rückkehrkonfiguration durchzuführen und alle Einstellungen zu testen, bevor Sie SSO aktivieren.



Die Verwendung des Sandbox-Modus ist sehr empfehlenswert, aber nicht unbedingt erforderlich. Wenn Sie bereit sind, AD FS zu erstellen, auf denen die Teilnehmer vertrauen, unmittelbar nach der Konfiguration von SSO in StorageGRID, Und Sie müssen die SSO- und SLO-Prozesse (Single Logout) für jeden Admin-Knoten nicht testen, klicken Sie auf **aktiviert**, geben Sie die StorageGRID-Einstellungen ein, erstellen Sie für jeden Admin-Knoten in AD FS ein Vertrauensverhältnis, und klicken Sie dann auf **Speichern**, um SSO zu aktivieren.

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei die Option **deaktiviertes** ausgewählt ist.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Save



Wenn die Optionen für den SSO-Status nicht angezeigt werden, bestätigen Sie, dass Sie Active Directory als föderierte Identitätsquelle konfiguriert haben. Siehe „Anforderungen für die Verwendung von Single Sign-On.“

2. Wählen Sie die Option **Sandbox Mode**.

Die Einstellungen für Identitäts-Provider und vertrauende Partei werden angezeigt. Im Abschnitt „Identitätsanbieter“ wird das Feld **Diensttyp** schreibgeschützt angezeigt. Es zeigt den Typ des Services zur Identitätsföderation an, den Sie verwenden (z. B. Active Directory).

3. Im Abschnitt „Identitätsanbieter“:

- a. Geben Sie den Namen des Föderationsdienstes ein, genau wie er in AD FS angezeigt wird.



Um den Federationsdienstnamen zu finden, gehen Sie zu Windows Server Manager. Wählen Sie **Tools > AD FS Management**. Wählen Sie im Menü Aktion die Option **Eigenschaften des Föderationsdienstes bearbeiten** aus. Der Name des Föderationsdienstes wird im zweiten Feld angezeigt.

- b. Geben Sie an, ob Sie die Verbindung mit Transport Layer Security (TLS) sichern möchten, wenn der Identitäts-Provider SSO-Konfigurationsinformationen als Antwort auf StorageGRID-Anforderungen sendet.

- **Verwenden Sie das Betriebssystem CA-Zertifikat:** Verwenden Sie das auf dem Betriebssystem installierte Standard-CA-Zertifikat, um die Verbindung zu sichern.
- **Benutzerdefiniertes CA-Zertifikat verwenden:** Verwenden Sie ein benutzerdefiniertes CA-Zertifikat, um die Verbindung zu sichern.

Wenn Sie diese Einstellung auswählen, kopieren Sie das Zertifikat in das Textfeld **CA-Zertifikat** und fügen es ein.

- **Verwenden Sie keine TLS:** Verwenden Sie kein TLS-Zertifikat, um die Verbindung zu sichern.

4. Geben Sie im Abschnitt „Vertrauenspartei“ die ID der betreffenden Partei an, die Sie für StorageGRID-Admin-Knoten verwenden, wenn Sie Vertrauensstellungen der betreffenden Partei konfigurieren.

- Wenn Ihr Grid beispielsweise nur einen Admin-Node hat und Sie nicht erwarten, dass künftig weitere Admin-Nodes hinzugefügt werden, geben Sie ein `SG` Oder `StorageGRID`.
- Wenn Ihr Grid mehr als einen Admin-Node enthält, fügen Sie die Zeichenfolge ein `[HOSTNAME]` In der Kennung. Beispiel: `SG-[HOSTNAME]`. Dadurch wird eine Tabelle mit einer auf den Hostnamen des Knotens beruhenden Partei-ID für jeden Admin-Node generiert. + HINWEIS: Sie müssen eine Vertrauensbasis für jeden Admin-Knoten in Ihrem StorageGRID-System erstellen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

5. Klicken Sie Auf **Speichern**.

- Ein grünes Häkchen wird für einige Sekunden auf der Schaltfläche **Speichern** angezeigt.



- Der Bestätigungshinweis zum Sandbox-Modus wird angezeigt und bestätigt, dass der Sandbox-Modus nun aktiviert ist. Sie können diesen Modus verwenden, während Sie AD FS verwenden, um ein

Vertrauensverhältnis von Vertrauensstellen für jeden Admin-Node zu konfigurieren und die Single Sign-in (SSO)- und SLO-Prozesse (Single Logout) zu testen.

Single Sign-on

You can enable single sign-on (SSO) if you want an external identity provider (IdP) to authorize all user access to StorageGRID. To start, enable [identity federation](#) and confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts. Next, select Sandbox Mode to configure, save, and then test your SSO settings. After verifying the connections, select Enabled and click Save to start using SSO.

SSO Status Disabled Sandbox Mode Enabled

Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/adfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

Verwandte Informationen

["Anforderungen für die Nutzung von Single Sign On"](#)

Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS

Sie müssen Active Directory Federation Services (AD FS) verwenden, um ein Vertrauensverhältnis für jeden Admin-Knoten in Ihrem System zu erstellen. Sie können vertraut mit PowerShell-Befehlen erstellen, SAML-Metadaten von StorageGRID importieren oder die Daten manuell eingeben.

Erstellen eines Vertrauensverhältnisses mit Windows PowerShell

Mit Windows PowerShell können Sie schnell ein oder mehrere Vertrauensstellen von vertrauenswürdigen Parteien erstellen.

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domännennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.

- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

1. Klicken Sie im Windows-Startmenü mit der rechten Maustaste auf das PowerShell-Symbol und wählen Sie **als Administrator ausführen** aus.
2. Geben Sie an der PowerShell-Eingabeaufforderung den folgenden Befehl ein:

```
Add-AdfsRelyingPartyTrust -Name "Admin_Node_Identifer" -MetadataURL  
"https://Admin_Node_FQDN/api/saml-metadata"
```

- Für *Admin_Node_Identifer*, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: SG-DC1-ADM1.
 - Für *Admin_Node_FQDN*, Geben Sie den vollständig qualifizierten Domännennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)
3. Wählen Sie im Windows Server Manager **Tools > AD FS Management** aus.

Das AD FS Management Tool wird angezeigt.

4. Wählen Sie **AD FS > vertraut auf Partei**.

Die Liste der Vertrauensstellen wird angezeigt.

5. Fügen Sie eine Zugriffskontrollrichtlinie zum neu erstellten Vertrauen der Vertrauensstellenden Partei hinzu:
 - a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
 - b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Zugriffskontrollrichtlinie bearbeiten**.
 - c. Wählen Sie eine Zugriffskontrollrichtlinie aus.
 - d. Klicken Sie auf **Anwenden** und klicken Sie auf **OK**
6. Fügen Sie dem neu erstellten Treuhandgesellschaft eine Richtlinie zur Ausstellung von Forderungen hinzu:
 - a. Suchen Sie das Vertrauen der Vertrauensgesellschaft, das Sie gerade erstellt haben.
 - b. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
 - c. Klicken Sie auf **Regel hinzufügen**.
 - d. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
 - e. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.

- f. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - g. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
 - h. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
 - i. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.
7. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.
- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
 - b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.
- Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.
8. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
9. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück ["Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen"](#) Um sicherzustellen, dass sie richtig konfiguriert sind.

Schaffung eines Vertrauensverhältnisses durch den Import von Federationmetadaten

Sie können die Werte für jedes Vertrauen der betreffenden Anbieter importieren, indem Sie für jeden Admin-Node auf die SAML-Metadaten zugreifen.

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domännennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

1. Klicken Sie im Windows Server Manager auf **Tools** und wählen Sie dann **AD FS Management** aus.
2. Klicken Sie unter Aktionen auf **Vertrauensstellung hinzufügen**.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus und klicken Sie auf **Start**.
4. Wählen Sie **Daten über die online veröffentlichte oder auf einem lokalen Netzwerk** importieren.

5. Geben Sie unter **Federation Metadatenadresse (Hostname oder URL)** den Speicherort der SAML-Metadaten für diesen Admin-Node ein:

`https://Admin_Node_FQDN/api/saml-metadata`

Für *Admin_Node_FQDN*, Geben Sie den vollständig qualifizierten Domännennamen für denselben Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

6. Schließen Sie den Assistenten „Vertrauen in die Vertrauensstellung“, speichern Sie das Vertrauen der vertrauenden Partei und schließen Sie den Assistenten.



Verwenden Sie bei der Eingabe des Anzeigenamens die bevertrauende Partei-ID für den Admin-Node genau so, wie sie auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1.

7. Fügen Sie eine Antragsregel hinzu:

- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.
- b. Klicken Sie auf **Regel hinzufügen**:
- c. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
- d. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.

- e. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
- f. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
- g. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
- h. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.

8. Bestätigen Sie, dass die Metadaten erfolgreich importiert wurden.

- a. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
- b. Vergewissern Sie sich, dass die Felder auf den Registerkarten **Endpunkte**, **Identifizier** und **Signatur** ausgefüllt sind.

Wenn die Metadaten fehlen, bestätigen Sie, dass die Federation-Metadatenadresse korrekt ist, oder geben Sie einfach die Werte manuell ein.

9. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.

10. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück ["Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen"](#) Um sicherzustellen, dass sie richtig konfiguriert sind.

Manuelles Erstellen eines Vertrauensverhältnisses mit einer Vertrauensbasis

Wenn Sie sich entscheiden, die Daten für die Treuhanddienste des Treuhandteils nicht zu importieren, können Sie die Werte manuell eingeben.

Was Sie benötigen

- Sie haben SSO in StorageGRID konfiguriert, und Sie kennen den vollständig qualifizierten Domänennamen (oder die IP-Adresse) und die bestellte Partei-ID für jeden Admin-Node in Ihrem System.



Sie müssen für jeden Admin-Knoten in Ihrem StorageGRID-System ein Vertrauensverhältnis aufbauen. Mit einer Vertrauensbasis für jeden Admin-Knoten wird sichergestellt, dass Benutzer sich sicher bei und aus jedem Admin-Knoten anmelden können.

- Sie haben das benutzerdefinierte Zertifikat, das für die StorageGRID Managementoberfläche hochgeladen wurde, oder Sie wissen, wie Sie sich von der Command Shell bei einem Admin-Node einloggen.
- Sie haben Erfahrung beim Erstellen von Vertrauensstellungen von Vertrauensstellen in AD FS, oder Sie haben Zugriff auf die Microsoft AD FS-Dokumentation.
- Sie verwenden das Snap-in AD FS Management und gehören der Gruppe Administratoren an.

Über diese Aufgabe

Diese Anweisungen gelten für AD FS 4.0, das in Windows Server 2016 enthalten ist. Wenn Sie AD FS 3.0 verwenden, das in Windows 2012 R2 enthalten ist, werden Sie leichte Unterschiede feststellen. Wenn Sie Fragen haben, lesen Sie bitte die Microsoft AD FS-Dokumentation.

Schritte

1. Klicken Sie im Windows Server Manager auf **Tools** und wählen Sie dann **AD FS Management** aus.
2. Klicken Sie unter Aktionen auf **Vertrauensstellung hinzufügen**.
3. Wählen Sie auf der Begrüßungsseite * Claims Aware* aus und klicken Sie auf **Start**.
4. Wählen Sie **Geben Sie Daten über den Kunden manuell** ein, und klicken Sie auf **Weiter**.
5. Schließen Sie den Assistenten für Vertrauen in die vertrauende Partei ab:

- a. Geben Sie einen Anzeigenamen für diesen Admin-Node ein.

Verwenden Sie für Konsistenz den Admin-Node mit der bewirtenden Partei-Kennung, genau wie er auf der Seite Single Sign-On im Grid Manager angezeigt wird. Beispiel: SG-DC1-ADM1.

- b. Überspringen Sie den Schritt, um ein optionales Token-Verschlüsselungszertifikat zu konfigurieren.
- c. Aktivieren Sie auf der Seite „URL konfigurieren“ das Kontrollkästchen **Unterstützung für das SAML 2.0 WebSSO-Protokoll** aktivieren.
- d. Geben Sie die Endpunkt-URL des SAML-Service für den Admin-Node ein:

`https://Admin_Node_FQDN/api/saml-response`

Für `Admin_Node_FQDN` Geben Sie den vollständig qualifizierten Domänennamen für den Admin-Knoten ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

- e. Geben Sie auf der Seite Configure Identifiers die befolgende Partei-ID für denselben Admin-Node an:

Admin_Node_Identifier

Für *Admin_Node_Identifier*, Geben Sie die ID für den Admin-Knoten auf, die sich auf der Seite Single Sign-On befindet, genau so ein, wie sie auf der Seite „Single Sign-On“ angezeigt wird. Beispiel: SG-DC1-ADM1.

- f. Überprüfen Sie die Einstellungen, speichern Sie das Vertrauen der Vertrauensstellungsgesellschaft, und schließen Sie den Assistenten.

Das Dialogfeld „Forderungsrichtlinie bearbeiten“ wird angezeigt.



Wenn das Dialogfeld nicht angezeigt wird, klicken Sie mit der rechten Maustaste auf das Vertrauen und wählen Sie **Richtlinie zur Bearbeitung von Forderungen** aus.

6. Um den Assistenten für die Antragsregel zu starten, klicken Sie auf **Regel hinzufügen**:
 - a. Wählen Sie auf der Seite Regelvorlage auswählen in der Liste **LDAP-Attribute als Ansprüche senden** aus, und klicken Sie auf **Weiter**.
 - b. Geben Sie auf der Seite Regel konfigurieren einen Anzeigenamen für diese Regel ein.

Beispiel: **ObjectGUID an Name ID**.
 - c. Wählen Sie im Attributspeicher die Option **Active Directory** aus.
 - d. Geben Sie in der Spalte LDAP-Attribut der Mapping-Tabelle **objectGUID** ein.
 - e. Wählen Sie in der Spalte Abgehender Antragstyp der Zuordnungstabelle in der Dropdown-Liste **Name ID** aus.
 - f. Klicken Sie auf **Fertig stellen**, und klicken Sie auf **OK**.
7. Klicken Sie mit der rechten Maustaste auf das Vertrauen der Vertrauenssteller, um seine Eigenschaften zu öffnen.
8. Konfigurieren Sie auf der Registerkarte **Endpunkte** den Endpunkt für einzelne Abmeldung (SLO):
 - a. Klicken Sie auf **SAML hinzufügen**.
 - b. Wählen Sie **Endpunkttyp > SAML Logout**.
 - c. Wählen Sie **Bindung > Umleiten**.
 - d. Geben Sie im Feld **Trusted URL** die URL ein, die für Single Logout (SLO) von diesem Admin-Node verwendet wird:

`https://Admin_Node_FQDN/api/saml-logout`

Für *Admin_Node_FQDN*, Geben Sie den vollständig qualifizierten Domännennamen des Admin-Knotens ein. (Bei Bedarf können Sie stattdessen die IP-Adresse des Node verwenden. Wenn Sie hier jedoch eine IP-Adresse eingeben, beachten Sie, dass Sie dieses Vertrauen der Vertrauensbasis aktualisieren oder neu erstellen müssen, wenn sich diese IP-Adresse immer ändert.)

- a. Klicken Sie auf **OK**.
9. Geben Sie auf der Registerkarte **Signatur** das Signaturzertifikat für dieses Vertrauen der bevertrauenden Partei an:
 - a. Fügen Sie das benutzerdefinierte Zertifikat hinzu:
 - Wenn Sie über das benutzerdefinierte Managementzertifikat verfügen, das Sie in StorageGRID

hochgeladen haben, wählen Sie dieses Zertifikat aus.

- Wenn Sie nicht über das benutzerdefinierte Zertifikat verfügen, melden Sie sich beim Admin-Knoten an, gehen Sie zu `/var/local/mgmt-api` Verzeichnis des Admin-Knotens, und fügen Sie das hinzu `custom-server.crt` Zertifikatdatei.

Hinweis: das Standardzertifikat des Admin-Knotens verwenden (`server.crt`) Wird nicht empfohlen. Wenn der Admin-Knoten ausfällt, wird das Standardzertifikat neu generiert, wenn Sie den Knoten wiederherstellen, und Sie müssen das Vertrauen der Vertrauensstelle aktualisieren.

- b. Klicken Sie auf **Anwenden** und klicken Sie auf **OK**.

Die Eigenschaften der zu vertrauenden Partei werden gespeichert und geschlossen.

10. Wiederholen Sie diese Schritte, um ein Vertrauensverhältnis für alle Administratorknoten in Ihrem StorageGRID-System zu konfigurieren.
11. Wenn Sie fertig sind, kehren Sie zu StorageGRID und zurück "[Testen Sie alle Vertrauensstellen, die sich auf die Vertrauensstellen verlassen](#)" Um sicherzustellen, dass sie richtig konfiguriert sind.

Testen von Vertrauen von Vertrauensstellen

Bevor Sie die Verwendung von Single Sign On (SSO) für StorageGRID durchsetzen, müssen Sie sicherstellen, dass Single Sign On und Single Logout (SLO) korrekt konfiguriert sind. Wenn Sie für jeden Admin-Node eine Vertrauensbasis erstellt haben, bestätigen Sie, dass Sie SSO und SLO für jeden Admin-Node verwenden können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.
- Sie haben eine oder mehrere Vertrauensstellen in AD FS konfiguriert.

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei die Option **Sandbox Mode** ausgewählt ist.

2. Suchen Sie in den Anweisungen für den Sandbox-Modus den Link zur Anmeldeseite Ihres Identitätsanbieters.

Die URL wird aus dem Wert abgeleitet, den Sie im Feld **Federated Service Name** eingegeben haben.

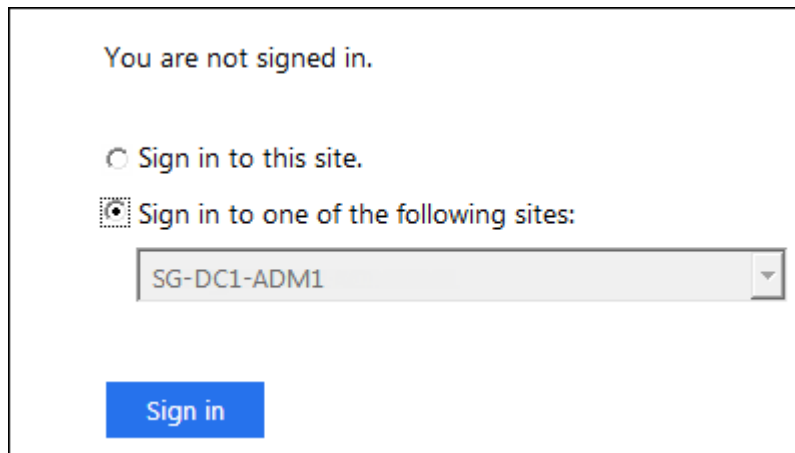
Sandbox mode

Sandbox mode is currently enabled. Use this mode to configure relying party trusts and to confirm that single sign-on (SSO) and single logout (SLO) are correctly configured for the StorageGRID system.

1. Use Active Directory Federation Services (AD FS) to create relying party trusts for StorageGRID. Create one trust for each Admin Node, using the relying party identifier(s) shown below.
2. Go to your identity provider's sign-on page: <https://ad2016.saml.sgws/dfs/ls/idpinitiatedsignon.htm>
3. From this page, sign in to each StorageGRID relying party trust. If the SSO operation is successful, StorageGRID displays a page with a success message. Otherwise, an error message is displayed.

When you have confirmed SSO for each of the relying party trusts and you are ready to enforce the use of SSO for StorageGRID, change the SSO Status to Enabled, and click Save.

3. Klicken Sie auf den Link oder kopieren Sie die URL in einen Browser, um auf die Anmeldeseite Ihres Identitätsanbieters zuzugreifen.
4. Um zu bestätigen, dass Sie SSO zur Anmeldung bei StorageGRID verwenden können, wählen Sie **Anmelden bei einer der folgenden Sites**, wählen Sie die vertrauenswürdige Partei-ID für Ihren primären Admin-Knoten und klicken Sie auf **Anmelden**.



The screenshot shows a sign-in interface. At the top, it says "You are not signed in." Below this, there are two radio buttons: "Sign in to this site." (which is unselected) and "Sign in to one of the following sites:" (which is selected). Under the selected option, there is a dropdown menu with "SG-DC1-ADM1" selected. At the bottom left, there is a blue "Sign in" button.

Sie werden aufgefordert, Ihren Benutzernamen und Ihr Kennwort einzugeben.

5. Geben Sie Ihren föderierten Benutzernamen und Ihr Kennwort ein.
 - Wenn die SSO-Anmelde- und -Abmeldevorgänge erfolgreich sind, wird eine Erfolgsmeldung angezeigt.

✓ Single sign-on authentication and logout test completed successfully.

- Wenn der SSO-Vorgang nicht erfolgreich ist, wird eine Fehlermeldung angezeigt. Beheben Sie das Problem, löschen Sie die Cookies des Browsers, und versuchen Sie es erneut.
6. Wiederholen Sie die vorherigen Schritte, um zu bestätigen, dass Sie sich bei anderen Admin-Nodes anmelden können.

Wenn alle SSO-Anmelde- und Abmeldevorgänge erfolgreich sind, können Sie SSO aktivieren.

Aktivieren von Single Sign On

Nachdem Sie den Sandbox-Modus verwendet haben, um alle Trusts von StorageGRID-Kunden zu testen, sind Sie bereit, Single Sign-On (SSO) zu aktivieren.

Was Sie benötigen

- Sie müssen mindestens eine föderierte Gruppe aus der Identitätsquelle importiert und der Gruppe Root Access Management-Berechtigungen zugewiesen haben. Sie müssen bestätigen, dass mindestens ein verbundener Benutzer Root Access-Berechtigung für den Grid Manager und den Tenant Manager für alle bestehenden Mandantenkonten hat.
- Sie müssen alle Vertrauensstellen der Vertrauensbesteller mit Sandbox-Modus getestet haben.

Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt, wobei **Sandbox-Modus** ausgewählt ist.

2. Ändern Sie den SSO-Status in **aktiviert**.
3. Klicken Sie Auf **Speichern**.

Es wird eine Warnmeldung angezeigt.

Warning

Enable single sign-on

After you enable SSO, no local users—including the root user—will be able to sign in to the Grid Manager, the Tenant Manager, the Grid Management API, or the Tenant Management API.

Before proceeding, confirm the following:

- You have imported at least one federated group from the identity source and assigned Root Access management permissions to the group. You must confirm that at least one federated user has Root Access permission to the Grid Manager and to the Tenant Manager for any existing tenant accounts.
- You have tested all relying party trusts using sandbox mode.

Are you sure you want to enable single sign-on?

Cancel

OK

4. Überprüfen Sie die Warnung und klicken Sie auf **OK**.

Single Sign-On ist jetzt aktiviert.



Alle Benutzer müssen SSO verwenden, um auf den Grid Manager, den Mandanten-Manager, die Grid-Management-API und die Mandanten-Management-API zuzugreifen. Lokale Benutzer können nicht mehr auf StorageGRID zugreifen.

Deaktivieren der Einzelanmeldung

Sie können Single Sign-On (SSO) deaktivieren, wenn Sie diese Funktion nicht mehr verwenden möchten. Sie müssen Single Sign-On deaktivieren, bevor Sie die Identitätsföderation deaktivieren können.

Was Sie benötigen

- Sie müssen über einen unterstützten Browser beim Grid Manager angemeldet sein.
- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

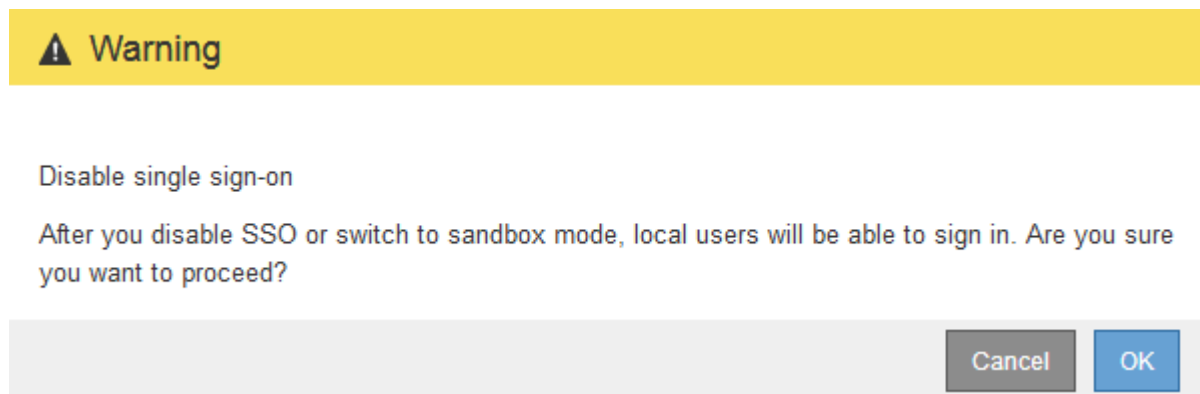
Schritte

1. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.

Die Seite Single Sign-On wird angezeigt.

2. Wählen Sie die Option **deaktiviert** aus.
3. Klicken Sie Auf **Speichern**.

Es wird eine Warnmeldung angezeigt, die darauf hinweist, dass lokale Benutzer sich jetzt anmelden können.



4. Klicken Sie auf **OK**.

Wenn Sie sich das nächste Mal bei StorageGRID anmelden, wird die Seite StorageGRID-Anmeldung angezeigt. Sie müssen den Benutzernamen und das Kennwort für einen lokalen oder föderierten StorageGRID-Benutzer eingeben.

Vorübergehend deaktivieren und erneut aktivieren der Single Sign-On für einen Admin-Knoten

Sie können sich möglicherweise nicht beim Grid-Manager anmelden, wenn das SSO-System (Single Sign-On) ausfällt. In diesem Fall können Sie SSO für einen Admin-Node vorübergehend deaktivieren und erneut aktivieren. Um SSO zu deaktivieren und dann erneut zu aktivieren, müssen Sie auf die Befehlshaber des Node zugreifen.

Was Sie benötigen

- Sie müssen über spezifische Zugriffsberechtigungen verfügen.

- Sie müssen die haben `Passwords.txt` Datei:
- Sie müssen das Passwort für den lokalen Root-Benutzer kennen.

Über diese Aufgabe

Nachdem Sie SSO für einen Admin-Node deaktiviert haben, können Sie sich beim Grid-Manager als lokaler Root-Benutzer anmelden. Zum Sichern Ihres StorageGRID-Systems müssen Sie die Befehlshaber des Node verwenden, um SSO auf dem Admin-Node erneut zu aktivieren, sobald Sie sich abmelden.



Das Deaktivieren von SSO für einen Admin-Node wirkt sich nicht auf die SSO-Einstellungen für andere Admin-Nodes im Raster aus. Das Kontrollkästchen **SSO aktivieren** auf der Seite Single Sign-On im Grid Manager bleibt aktiviert, und alle vorhandenen SSO-Einstellungen bleiben erhalten, wenn Sie sie nicht aktualisieren.

Schritte

1. Melden Sie sich bei einem Admin-Knoten an:
 - a. Geben Sie den folgenden Befehl ein: `ssh admin@Admin_Node_IP`
 - b. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:
 - c. Geben Sie den folgenden Befehl ein, um zum Root zu wechseln: `su -`
 - d. Geben Sie das im aufgeführte Passwort ein `Passwords.txt` Datei:

Wenn Sie als root angemeldet sind, ändert sich die Eingabeaufforderung von `$` Bis `#`.

2. Führen Sie den folgenden Befehl aus: `disable-saml`

Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

3. Bestätigen Sie, dass Sie SSO deaktivieren möchten.

Eine Meldung gibt an, dass Single Sign-On auf dem Knoten deaktiviert ist.

4. Greifen Sie über einen Webbrowser auf den Grid Manager auf demselben Admin-Node zu.

Die Anmeldeseite für den Grid Manager wird jetzt angezeigt, weil SSO deaktiviert wurde.

5. Melden Sie sich mit dem Benutzernamen root und dem Passwort des lokalen Root-Benutzers an.
6. Wenn Sie SSO vorübergehend deaktiviert haben, da Sie die SSO-Konfiguration korrigieren mussten:
 - a. Wählen Sie **Konfiguration > Zugriffskontrolle > Single Sign-On**.
 - b. Ändern Sie die falschen oder veralteten SSO-Einstellungen.
 - c. Klicken Sie Auf **Speichern**.

Wenn Sie auf der Seite Single Sign-On auf **Save** klicken, wird SSO für das gesamte Raster automatisch wieder aktiviert.

7. Wenn Sie SSO vorübergehend deaktiviert haben, weil Sie aus einem anderen Grund auf den Grid Manager zugreifen mussten:
 - a. Führen Sie alle Aufgaben oder Aufgaben aus, die Sie ausführen müssen.
 - b. Klicken Sie auf **Abmelden** und schließen Sie den Grid Manager.

c. SSO auf dem Admin-Node erneut aktivieren. Sie können einen der folgenden Schritte ausführen:

- Führen Sie den folgenden Befehl aus: `enable-saml`

Eine Meldung gibt an, dass der Befehl nur für diesen Admin-Knoten gilt.

Bestätigen Sie, dass Sie SSO aktivieren möchten.

Eine Meldung gibt an, dass Single Sign-On auf dem Knoten aktiviert ist.

- Booten Sie den Grid-Node neu: `reboot`

8. Greifen Sie über einen Webbrowser über denselben Admin-Node auf den Grid-Manager zu.

9. Vergewissern Sie sich, dass die Seite StorageGRID-Anmeldung angezeigt wird und Sie Ihre SSO-Anmeldedaten für den Zugriff auf den Grid-Manager eingeben müssen.

Verwandte Informationen

["Konfigurieren der Single Sign-On-Konfiguration"](#)

Copyright-Informationen

Copyright © 2024 NetApp. Alle Rechte vorbehalten. Gedruckt in den USA. Dieses urheberrechtlich geschützte Dokument darf ohne die vorherige schriftliche Genehmigung des Urheberrechtinhabers 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, BEISPIELHAFT 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 IRGEND EINER 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.