Zugriff auf den SP/BMC

ONTAP 9

NetApp
March 21, 2023

Inhaltsverzeichnis

Zugriff auf den SP/BMC

Konten, die auf den SP zugreifen können

Wenn Sie versuchen, auf den SP zuzugreifen, werden Sie nach Berechtigungen gefragt. Cluster-Benutzerkonten, die mit dem erstellt werden `service-processor` Applikationstyp hat Zugriff auf die SP-CLI auf jedem Node des Clusters. SP-Benutzerkonten werden über ONTAP verwaltet und per Passwort authentifiziert. Ab ONTAP 9.9 müssen die SP-Benutzerkonten über den verfügen `admin` Rolle:

Benutzerkonten für den Zugriff auf den SP werden über ONTAP statt über die SP-CLI verwaltet. Ein Cluster-Benutzerkonto kann auf den SP zugreifen, wenn es mit dem erstellt wird `-application` Parameter von `security login create` Befehl ist auf festgelegt `service-processor` Und das `-authmethod` Parameter auf gesetzt `password`. Der SP unterstützt nur die Passwort-Authentifizierung.

Sie müssen das angeben `-role` Parameter beim Erstellen eines SP-Benutzerkontos.

- In ONTAP 9.9.1 und höheren Versionen müssen Sie angeben `admin` Für das `-role` Parameter und alle Änderungen an einem Konto erfordern das `admin` Rolle: Andere Rollen sind aus Sicherheitsgründen nicht mehr zulässig.
  - Wenn Sie ein Upgrade auf ONTAP 9.9.1 oder neuere Versionen durchführen, lesen Sie "Ändern von Benutzerkonten, die auf den Service Processor zugreifen können".
  - Beim Wechsel zurück zu ONTAP 9.8 oder älteren Versionen finden Sie Informationen unter "Überprüfen Sie, ob Benutzerkonten, die auf den Service Processor zugreifen können".
- In ONTAP 9.8 und älteren Versionen kann jede Rolle jedoch auf den SP zugreifen `admin` Wird empfohlen.

Standardmäßig enthält das Cluster-Benutzerkonto mit dem Namen „`admin`“ das `service-processor` Applikationstyp und hat Zugriff auf den SP.

ONTAP verhindert, dass Sie Benutzerkonten mit Namen erstellen, die für das System reserviert sind (z. B. „`root`“ und „`naroot`“). Sie können keinen systemreservierten Namen für den Zugriff auf das Cluster oder den SP verwenden.

Sie können aktuelle SP-Benutzerkonten mithilfe der anzeigen `-application service-processor` Parameter von `security login show` Befehl.

Greifen Sie von einem Administrationshost aus auf den SP/BMC zu

Sie können sich über einen Administrationshost beim SP eines Node einloggen, um Node-Managementaufgaben Remote auszuführen.

Was Sie benötigen

Folgende Bedingungen müssen erfüllt sein:

- Der Administrationshost, den Sie für den Zugriff auf den SP verwenden, muss SSHv2 unterstützen.
- Ihr Benutzerkonto muss bereits für den Zugriff auf den SP eingerichtet sein.

Für den Zugriff auf den SP muss Ihr Benutzerkonto mit dem erstellt worden sein `-application` Parameter von `security login create` Befehl ist auf festgelegt `service-processor` Und das `-authmethod` Parameter auf gesetzt `password`.

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Wenn der SP so konfiguriert ist, dass er eine IPv4- oder IPv6-Adresse verwendet, und wenn fünf SSH-Anmeldeversuche von einem Host innerhalb von 10 Minuten nacheinander fehlschlagen, weist der SP SSH-Anmeldeanfragen zurück und setzt die Kommunikation mit der IP-Adresse des Hosts 15 Minuten lang aus. Die Kommunikation wird nach 15 Minuten fortgesetzt, und Sie können versuchen, sich erneut beim SP anzumelden.

Mit ONTAP können Sie keine systemreservierten Namen (z. B. „`root`“ und „`naroot`“) für den Zugriff auf das Cluster oder den SP erstellen oder verwenden.

Schritte

1. Melden Sie sich vom Administrations-Host beim SP an:

   `ssh username@SP_IP_address`

2. Wenn Sie dazu aufgefordert werden, geben Sie das Passwort für ein `username`.

   Die SP-Eingabeaufforderung wird angezeigt. Hier wird angegeben, dass Sie auf die SP-CLI zugreifen können.

Beispiele für SP-Zugriff von einem Administrationshost aus

Im folgenden Beispiel wird gezeigt, wie Sie sich mit einem Benutzerkonto beim SP einloggen `joe`, Die für den Zugriff auf den SP eingerichtet wurde.

```
[admin_host]$ ssh joe@192.168.123.98
joe@192.168.123.98's password:
SP>
```

In den folgenden Beispielen wird veranschaulicht, wie Sie sich bei einem Node, auf dem SSH für IPv6 eingerichtet ist, mit der globalen IPv6-Adresse oder über den IPv6-Router angekündigte Adresse beim SP einloggen.

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202::1234
joe@fd22:8b1e:b255:202::1234's password:
SP>
```

```
[admin_host]$ ssh joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b
joe@fd22:8b1e:b255:202:2a0:98ff:fe01:7d5b's password:
SP>
```

Greifen Sie über die Systemkonsole auf den SP/BMC zu

Sie können über die Systemkonsole (auch „*serial Console*“) auf den SP zugreifen, um Überwachungs- oder Fehlerbehebungsaufgaben durchzuführen.

Über diese Aufgabe

Diese Aufgabe gilt sowohl für den SP als auch für den BMC.

Schritte

1. Greifen Sie von der Systemkonsole auf die SP-CLI zu, indem Sie an der Eingabeaufforderung Strg-G drücken.
2. Melden Sie sich bei der SP-CLI an, wenn Sie dazu aufgefordert werden.

   Die SP-Eingabeaufforderung wird angezeigt. Hier wird angegeben, dass Sie auf die SP-CLI zugreifen können.

3. Beenden Sie die SP-CLI und kehren Sie zur Systemkonsole zurück, indem Sie Strg-D drücken und dann die Eingabetaste drücken.

Beispiel für den Zugriff auf die SP-CLI von der Systemkonsole

Im folgenden Beispiel werden die Ergebnisse beim Drücken von Strg-G von der Systemkonsole angezeigt, um auf die SP-CLI zuzugreifen. Der `help system power` Der Befehl wird an der SP-Eingabeaufforderung eingegeben, gefolgt von Strg-D und anschließend mit der Eingabetaste zur Systemkonsole.

```
cluster1::>
```

(Drücken Sie Strg-G, um auf die SP-CLI zuzugreifen.)

```
Switching console to Service Processor
Service Processor Login:
Password:
SP>
SP> help system power
system power cycle - power the system off, then on
system power off - power the system off
system power on - power the system on
system power status - print system power status
SP>
```

(Drücken Sie Strg-D und anschließend die Eingabetaste, um zur Systemkonsole zurückzukehren.)

```
cluster1::>
```

Beziehung zwischen der SP-CLI, der SP-Konsole und den Systemkonsolensitzungen

Sie können eine SP-CLI-Session öffnen, um einen Node Remote zu verwalten, und eine separate SP-Konsolensitzung öffnen, um auf die Konsole des Node zuzugreifen. Die SP-Konsolensitzung spiegelt die Ausgabe, die in einer gleichzeitigen Systemkonsolensitzung angezeigt wird. Der SP und die Systemkonsole verfügen über unabhängige Shell-Umgebungen mit unabhängiger Anmeldeauthentifizierung.

Wenn Sie Allgemeines zur SP-CLI, zur SP-Konsole und zu Systemkonsolensitzungen tun, können Sie einen Node Remote verwalten. Im Folgenden wird die Beziehung zwischen den Sitzungen beschrieben:

- Nur ein Administrator kann sich gleichzeitig bei der SP-CLI-Sitzung anmelden. Mit dem SP können Sie jedoch sowohl eine SP-CLI-Sitzung als auch eine separate SP-Konsolensitzung öffnen.

  Die SP-CLI wird mit der SP-Eingabeaufforderung angezeigt (`SP>`). In einer SP-CLI-Session können Sie den SP verwenden `system console` Befehl zum Starten einer SP-Konsolensitzung Gleichzeitig können Sie eine separate SP-CLI-Sitzung über SSH starten. Wenn Sie Strg-D drücken, um die SP-Konsolensitzung zu beenden, kehren Sie automatisch zur SP-CLI-Session zurück. Wenn eine SP-CLI-Session bereits vorhanden ist, werden Sie mit einer Meldung gefragt, ob Sie die vorhandene SP-CLI-Session beenden möchten. Wenn Sie „`y`“ eingeben, wird die vorhandene SP-CLI-Sitzung beendet und Sie können von der SP-Konsole zur SP-CLI zurückkehren. Diese Aktion wird im SP-Ereignisprotokoll aufgezeichnet.

  In einer ONTAP-CLI-Session, die über SSH verbunden ist, können Sie zur Systemkonsole eines Node wechseln, indem Sie die ONTAP ausführen `system node run-console` Befehl von einem anderen Node.

- Aus Sicherheitsgründen besitzen die SP-CLI-Session und die Systemkonsolensitzung eine unabhängige Anmeldeauthentifizierung.

  Wenn Sie eine SP-Konsolensitzung über die SP-CLI initiieren (über den SP) `system console` Befehl). Sie werden aufgefordert, die Anmeldeinformationen für die Systemkonsole einzugeben. Wenn Sie über eine Systemkonsolensession auf die SP-CLI zugreifen (durch Drücken von Strg-G), werden Sie nach den SP-CLI-Berechtigungen gefragt.

- Die SP-Konsolensitzung und die Systemkonsolensitzung verfügen über unabhängige Shell-Umgebungen.

  Die SP-Konsolensitzung spiegelt die Ausgabe, die in einer gleichzeitigen Systemkonsolensitzung angezeigt wird. Jedoch spiegelt die gleichzeitige Systemkonsolensitzung nicht die SP-Konsolensitzung.

  Die SP-Konsolensitzung spiegelt die Ausgabe gleichzeitiger SSH-Sessions nicht.

Verwalten Sie die IP-Adressen, die auf den SP zugreifen können

Standardmäßig akzeptiert der SP SSH-Verbindungsanfragen von Administrations-Hosts beliebiger IP-Adressen. Sie können den SP so konfigurieren, dass nur SSH-Verbindungsanforderungen von den Administrations-Hosts akzeptiert werden, die die angegebenen IP-Adressen haben. Die Änderungen, die Sie vornehmen, beziehen sich

auf SSH-Zugriff auf den SP aller Nodes im Cluster.

Schritte

1. Gewähren Sie SP-Zugriff nur auf die IP-Adressen, die Sie mit angeben `system service-processor ssh add-allowed-addresses` Befehl mit dem `-allowed-addresses` Parameter.
   - Der Wert des `-allowed-addresses` Der Parameter muss im Format von angegeben werden `address/netmask`, Und mehrfach `address/netmask` Paare müssen z. B. durch Kommas getrennt werden. `10.98.150.10/24, fd20:8b1e:b255:c09b::/64`.

     Einstellen des `-allowed-addresses` Parameter an `0.0.0.0/0, ::/0` Aktiviert alle IP-Adressen für den Zugriff auf den SP (Standard).

   - Wenn Sie die Standardeinstellung ändern, indem Sie den SP-Zugriff auf nur die von Ihnen angegebenen IP-Adressen beschränken, werden Sie von ONTAP aufgefordert, zu bestätigen, dass die angegebenen IP-Adressen die Standardeinstellung „`allow all`“ ersetzen sollen (`0.0.0.0/0, ::/0`).
   - Der `system service-processor ssh show` Mit dem Befehl werden die IP-Adressen angezeigt, die auf den SP zugreifen können.
2. Wenn Sie eine angegebene IP-Adresse vom Zugriff auf den SP blockieren möchten, verwenden Sie die `system service-processor ssh remove-allowed-addresses` Befehl mit dem `-allowed -addresses` Parameter.

   Wenn Sie alle IP-Adressen beim Zugriff auf den SP blockieren, kann auf den SP kein Administrations-Host mehr zugegriffen werden.

Beispiele für das Verwalten der IP-Adressen, die auf den SP zugreifen können

In den folgenden Beispielen wird die Standardeinstellung für SSH-Zugriff auf den SP angezeigt, die Standardeinstellung wird geändert, indem nur der SP-Zugriff auf die angegebenen IP-Adressen beschränkt wird, die angegebenen IP-Adressen aus der Zugriffsliste entfernt und dann der SP-Zugriff für alle IP-Adressen wiederhergestellt wird:

```
cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: The default "allow all" setting (0.0.0.0/0, ::/0) will be
replaced
         with your changes. Do you want to continue? {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: 192.168.1.202/24, 192.168.10.201/24

cluster1::> system service-processor ssh remove-allowed-addresses -allowed
-addresses 192.168.1.202/24, 192.168.10.201/24

Warning: If all IP addresses are removed from the allowed address list,
all IP
         addresses will be denied access. To restore the "allow all"
default,
         use the "system service-processor ssh add-allowed-addresses
         -allowed-addresses 0.0.0.0/0, ::/0" command. Do you want to
continue?
          {y|n}: y

cluster1::> system service-processor ssh show
  Allowed Addresses: -

cluster1::> system service-processor ssh add-allowed-addresses -allowed
-addresses 0.0.0.0/0, ::/0

cluster1::> system service-processor ssh show
  Allowed Addresses: 0.0.0.0/0, ::/0
```