Zugriff auf die Wartungskonsole für ONTAP Tools

ONTAP tools for VMware vSphere 9.10

NetApp
April 02, 2025

This PDF was generated from https://docs.netapp.com/de-de/ontap-tools-vmware-vsphere-910/manage/reference_maintenance_console_of_ontap_tools_for_vmware_vsphere.html on April 02, 2025. Always check docs.netapp.com for the latest.

Inhalt

Zugriff auf die Wartungskonsole für ONTAP Tools 1
Überblick über Wartungskonsole für ONTAP-Tools 1
Protokolldateien von Virtual Storage Console und VASA Provider 3
Ändern Sie das Administratorpasswort 3
Konfigurieren Sie VASA Provider für die Nutzung mit SSH 4
Konfigurieren Sie den Zugriff auf die Remote-Diagnose 4

Zugriff auf die Wartungskonsole für ONTAP Tools

Überblick über Wartungskonsole für ONTAP-Tools

Sie können Ihre Applikations-, System- und Netzwerkkonfigurationen mithilfe der Wartungskonsole der ONTAP Tools managen. Sie können Ihr Administratorkennwort und Ihr Wartungskennwort ändern. Außerdem können Sie Supportpakete generieren, verschiedene Protokollebenen festlegen, TLS-Konfigurationen anzeigen und verwalten und die Remote-Diagnose starten.

Sie müssen VMware-Tools installiert haben, nachdem Sie ONTAP-Tools implementiert haben, um auf die Wartungskonsole zuzugreifen. Sie sollten „`maint`“ als Benutzernamen und das Passwort verwenden, das Sie während der Bereitstellung konfiguriert haben, um sich an der Wartungskonsole der ONTAP-Tools anzumelden.

Sie müssen ein Passwort für den Benutzer „`diag`“ festlegen, während Sie die Ferndiagnose aktivieren.

Sie sollten über die Registerkarte „Übersicht“ der implementierten ONTAP Tools auf die Wartungskonsole zugreifen. Wenn Sie auf klicken , Die Wartungskonsole wird gestartet.

Konsolenmenü	Optionen
Anwendungskonfiguration	1. Zeigt eine Zusammenfassung des Serverstatus an 2. Starten Sie den Virtual Storage Console Service 3. Beenden Sie den Virtual Storage Console Service 4. Starten Sie VASA Provider und SRA Service 5. Beenden Sie den VASA Provider und den SRA Service 6. Ändern Sie das Benutzerpasswort „Administrator“ 7. Zertifikate erneut generieren 8. Hard Reset Key Store und Zertifikate 9. Hard Reset-Datenbank 10. ÄNDERN SIE DAS PROTOKOLL-Level für den Virtual Storage Console-Service 11. Ändern Sie DIE PROTOKOLLEBENE für den VASA Provider und den SRA Service 12. Anzeigen der TLS-Konfiguration 13. Aktivieren des TLS-Protokolls 14. Deaktivieren des TLS-Protokolls

Systemkonfiguration	1. Starten Sie die virtuelle Maschine neu 2. Virtuelle Maschine herunterfahren 3. Ändern Sie das Benutzerpasswort „Wartung“ 4. Zeitzone ändern 5. Fügen Sie den neuen NTP-Server hinzu Sie können eine IPv6-Adresse für Ihren NTP-Server angeben. 6. Aktivieren Sie SSH-Zugriff 7. Erhöhen der Größe der Jail-Festplatte (/jail) 8. Upgrade 9. Installation der VMware Tools
Netzwerkkonfiguration	1. Zeigt die Einstellungen für die IP-Adresse an 2. Ändern Sie die IP-Adresseinstellungen Sie können diese Option verwenden, um die IP-Adresse nach der Implementierung in IPv6 zu ändern. 3. Zeigen Sie die Einstellungen für die Suche nach Domain-Namen an 4. Ändern Sie die Einstellungen für die DNS-Suche 5. Statische Routen anzeigen 6. Ändern Sie statische Routen Sie können diese Option verwenden, um eine IPv6-Route hinzuzufügen. 7. Änderungen speichern 8. Ping an einen Host Sie können diese Option verwenden, um einen Ping an einen IPv6-Host zu senden. 9. Standardeinstellungen wiederherstellen
Support und Diagnose	1. Erzeugen Sie das Support Bundle 2. Zugriff auf die Diagnoseschale 3. Remote-Diagnosezugriff aktivieren

Protokolldateien von Virtual Storage Console und VASA Provider

Sie können die Protokolldateien im überprüfen `/opt/netapp/vscserver/log` Verzeichnis und das `/opt/netapp/vpserver/log` Verzeichnis, wenn Fehler auftreten.

Die folgenden drei Log-Dateien können bei der Identifizierung von Problemen hilfreich sein:

- `cxf.log`, Mit Informationen über API-Verkehr in und aus VASA Provider*`kaminoPrefs.xml`, Mit Informationen über VSC-Einstellungen
- `vvolvp.log`, Mit allen Protokollinformationen über VASA Provider

Im Wartungsmenü der ONTAP Tools für VMware vSphere können Sie unterschiedliche Log-Level für Ihre Anforderungen festlegen. Folgende Protokollebenen sind verfügbar:

- Info
- Debuggen
- Fehler
- Verfolgen

Wenn Sie die Protokollebenen festlegen, werden die folgenden Dateien aktualisiert:

- VSC-Server: `kamino.log` Und `vvolvp.log`
- VASA Provider-Server: `vvolvp.log`, `error.log`, und `netapp.log`

Darüber hinaus enthält die Seite über die Webbefehlszeilenschnittstelle (CLI) von VASA Provider die vorgemachten API-Aufrufe, die zurückgegebenen Fehler sowie mehrere Performance-bezogene Zähler. Die Web-CLI-Seite finden Sie unter `https://<IP_address_or_hostname>:9083/stats`.

Ändern Sie das Administratorpasswort

Sie können das Administratorpasswort der ONTAP-Tools nach der Implementierung mit der Wartungskonsole ändern.

Schritte

1. Öffnen Sie vom vCenter Server eine Konsole für die ONTAP Tools.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingabe `1` Wählen Sie in der Wartungskonsole Anwendungskonfiguration aus.
4. Eingabe `6`So wählen Sie **Administratorpasswort ändern** aus.
5. Geben Sie ein Passwort mit mindestens acht Zeichen und maximal 63 Zeichen ein.
6. Eingabe `y`Im Bestätigungsdialogfeld.

Konfigurieren Sie VASA Provider für die Nutzung mit SSH

Sie können den VASA Provider so einrichten, dass er SSH für den sicheren Zugriff verwendet, indem Sie die ONTAP-Tools konfigurieren.

Über diese Aufgabe

Wenn Sie SSH konfigurieren, müssen Sie sich als Benutzer für die Wartung einloggen. Der Grund dafür ist, dass der Root-Zugriff auf VASA Provider deaktiviert wurde. Wenn Sie andere Anmeldedaten verwenden, können Sie SSH nicht für den Zugriff auf VASA Provider verwenden.

Schritte

1. Öffnen Sie vom vCenter Server eine Konsole für die ONTAP Tools.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingabe `3` So wählen Sie **Systemkonfiguration** aus.
4. Eingabe `6` Wählen Sie **SSH-Zugriff aktivieren** aus.
5. Eingabe `y` Im Bestätigungsdialogfeld.

Konfigurieren Sie den Zugriff auf die Remote-Diagnose

Sie können die ONTAP-Tools konfigurieren, um SSH-Zugriff für den Diagnose-Benutzer zu aktivieren.

Was Sie brauchen

Die VASA Provider-Erweiterung muss für Ihre vCenter Server-Instanz aktiviert sein.

Über diese Aufgabe

Die Verwendung von SSH für den Zugriff auf das Diagnose-Benutzerkonto weist folgende Einschränkungen auf:

- Sie haben nur ein Anmeldekonto pro Aktivierung von SSH.
- SSH-Zugriff auf das Diagnose-Benutzerkonto ist deaktiviert, wenn eines der folgenden Ereignisse eintritt:
  - Die Zeit läuft ab.

    Die Anmeldesitzung bleibt nur bis Mitternacht am nächsten Tag gültig.
  - Sie melden sich erneut als Diagnose-Benutzer mit SSH an.

Schritte

1. Öffnen Sie über den vCenter Server eine Konsole für VASA Provider.
2. Melden Sie sich als Wartungbenutzer an.
3. Eingabe `4` Wählen Sie Support und Diagnose aus.
4. Eingabe `3` So wählen Sie den Zugriff auf Remote-Diagnose aktivieren aus.
5. Eingabe `y` Im Dialogfeld „Bestätigung“ können Sie den Remote-Diagnosezugriff aktivieren.

6. Geben Sie ein Kennwort für den Remote-Diagnosezugriff ein.

Copyright-Informationen

Copyright © 2025 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.