Note di rilascio di Sentinel 8.5

Agosto 2021

In Sentinel 8.5 sono stati risolti numerosi problemi esistenti e sono state aggiunte alcune nuove funzioni.

Molti miglioramenti sono stati apportati in base ai suggerimenti forniti dai clienti, che ringraziamo per la loro valida collaborazione. Confidiamo che anche in futuro continueranno ad aiutarci a migliorare i nostri prodotti affinché possano soddisfare tutte le loro esigenze. È possibile pubblicare commenti e opinioni nel forum di Sentinel, la nostra comunità online, che include anche informazioni sui prodotti, blog e collegamenti a risorse utili. È inoltre possibile condividere le idee per migliorare il prodotto sul portale delle idee.

La documentazione relativa a questo prodotto è disponibile in formato HTML e PDF, in una pagina a cui è possibile accedere senza eseguire il login. Se si desidera fornire suggerimenti su come migliorare la documentazione, fare clic sull'icona dei commenti in una pagina qualsiasi della versione HTML della documentazione pubblicata nella pagina relativa alla documentazione di Sentinel. Per effettuare il download di questo prodotto, visitare il sito Web di download del prodotto.

Novità

Nelle sezioni seguenti vengono illustrate le funzionalità principali fornite in questa versione, incluse le soluzioni ai problemi riscontrati:

Integrazione di ArcSight Intelligence con Sentinel

Questa versione fornisce ai clienti un modo per integrare Sentinel con le entusiasmanti tecnologie di analisi di ArcSight Intelligence. Pertanto, gli utenti di Sentinel possono ottenere il punteggio di rischio quasi in tempo reale e utilizzarlo per ulteriori analisi nelle proprie regole di correlazione e così via. Ciò consente a Sentinel di fornire un'esperienza ottimale nella ricerca delle minacce.

ArcSight Intelligence è una soluzione di analisi comportamentale di utenti ed entità che utilizza la scienza dei dati e le analisi avanzate per identificare le entità e i comportamenti più rischiosi all'interno dell'organizzazione. Intelligence stabilisce innanzitutto il normale comportamento delle entità organizzative, quindi utilizza l'analisi avanzata per identificare i comportamenti anomali di qualsiasi entità, fornendo un punteggio di rischio appropriato a ciascuna di queste entità.

Sentinel fornisce un metodo per l'integrazione con ArcSight Intelligence 6.3. Grazie a tale integrazione, per gli utenti di Sentinel sarà più semplice inviare i dati ad ArcSight Intelligence per l'analisi e sarà possibile ricevere i dettagli del punteggio di rischio delle entità da Intelligence. Ciò consente a Sentinel di rilevare gli utenti e le entità più a rischio nell'organizzazione che potrebbero compromettere l'intero sistema e creare una potenziale minaccia.

MITRE ATT&CK

MITRE ATT&CK aiuta i team di sicurezza informatica a valutare l'efficacia dei processi SOC (Security Operations Center) e ad adottare misure di difesa adeguate per identificare le aree di miglioramento. MITRE ATT&CK è una knowledge base accessibile a livello globale di tattiche e tecniche avversarie basate su osservazioni reali. La knowledge base di MITRE ATT&CK viene utilizzata come base per lo sviluppo di specifici modelli e metodologie di minacce nel settore privato, governativo e nella comunità di servizi e prodotti per la sicurezza informatica.

A partire da questa versione di Sentinel, gli amministratori possono mappare le regole di correlazione con l'ID MITRE ATT&CK. MITRE ATT&CK significa MITRE Adversarial Tattics, Techniques, and Common Knowledge (ATT&CK). Il MITRE ATT&CK Framework è un linguaggio comune del settore relativo alle tattiche e alle tecniche basate su osservazioni reali.

Gli amministratori di Sentinel possono ora mappare la propria regola di correlazione pronta all'uso o personalizzata direttamente con l'ID MITRE ATT&CK, fornendo un'analisi approfondita dei dati e consentendo di visualizzare quali regole vengono applicate o quali sono le tattiche e le tecniche MITRE sfruttate dai clienti. Sentinel fornisce agli amministratori un set di strumenti con cui possono ottenere immediatamente una panoramica della rete e di quali sono gli attacchi più importanti che devono prevenire.

Se viene attivata una regola di correlazione mappata a un ID MITRE ATT&CK, gli eventi attivati avranno l'ID MITRE ATT&CK e il nome MITRE ATT&CK. Questi eventi vengono analizzati tramite un widget disponibile in un dashboard di stato della sicurezza di default. I primi dieci nomi MITRE ATT&CK vengono visualizzati in questo dashboard nell'intervallo di tempo di 1 giorno e nell'intervallo di visualizzazione di 1 ora.

Upgrade del JDK

Per evitare vulnerabilità della sicurezza (CVE-2021-2161, CVE-2021-2163, CVE-2021-2341, CVE-2021-2432, CVE-2021-2369, CVE-2021-2388) e per utilizzare le funzioni di sicurezza dei nuovi standard JDK, viene eseguito l'upgrade del JDK dalla versione 1.8.0_update242 alla versione 1.8.0_update302

Memorizzazione degli eventi non elaborati provenienti dal connettore

Il connettore Syslog di Sentinel, a partire dalla versione 2021.1r1, consentirà di memorizzare gli eventi non elaborati provenienti dai connettori intelligenti ArcSight. Si tratta degli eventi originali e non processati che vengono generati direttamente dal dispositivo finale. Questa impostazione può essere abilitata selezionando l'opzione **Preserve Raw Event** (Conserva evento non elaborato) nel connettore intelligente corrispondente.

Supporto TLS

È stato rimosso il supporto a TLS 1.0 e TLS 1.1.

Versioni del sistema operativo (OS)

Installazione tradizionale: Sentinel è ora certificato anche per la seguente nuova piattaforma:

- Red Hat Enterprise Linux (RHEL) 8.3

Sistemi operativi obsoleti: in seguito alla rimozione del supporto da parte di RHEL e SLES, i seguenti sistemi operativi sono diventati obsoleti:

- RHEL 7.6 e 7.7
- SLES 15 SP1

Correzioni software

Sentinel 8.5 include correzioni software che risolvono i seguenti problemi:

- "La conversione in FIPS sul server Sentinel modifica il protocollo da TLS 1.2 a TLS 1.1" a pagina 3
- "Le chiamate REST di Sentinel hanno esito negativo dopo l'upgrade del client Java di Sentinel" a pagina 3
- "Errore durante la generazione di un nuovo rapporto" a pagina 3

La conversione in FIPS sul server Sentinel modifica il protocollo da TLS 1.2 a TLS 1.1

Problema: quando si esegue la conversione in FIPS sul server Sentinel, il protocollo viene modificato da TLS 1.2 a TLS 1.1, causando l'interruzione della connessione tra SAM e il server Sentinel. Tuttavia, il cliente deve utilizzare TLS 1.2

Correzione: ora quando si esegue la conversione a FIPS, la versione TLS non viene modificata da 1.2 a 1.1

Le chiamate REST di Sentinel hanno esito negativo dopo l'upgrade del client Java di Sentinel

Problema: dopo aver eseguito l'upgrade del client Java di Sentinel dalla versione 8.1 alla versione 8.2, le chiamate REST hanno esito negativo.

Correzione: ora dopo aver eseguito l'upgrade del client Java di Sentinel dalla versione 8.1 alla versione 8.2, le chiamate REST non hanno più esito negativo.

Errore durante la generazione di un nuovo rapporto

Problema: si verifica un errore durante la generazione di un nuovo rapporto. La causa principale dell'errore è la manomissione dell'archivio chiavi o una password non corretta.

Correzione: non si riceve più un errore durante la generazione di un nuovo rapporto.

Requisiti di sistema

Per ulteriori informazioni su requisiti hardware, sui sistemi operativi e sui browser supportati, vedere i Requisiti di sistema di Sentinel.

Informazioni sulla licenza e sull'acquisto

Per acquistare una licenza aziendale o eseguire l'upgrade della licenza esistente, chiamare il numero 1-800-529-3400, inviare un'e-mail all'indirizzo info@microfocus.com o visitare https://www.microfocus.com/it-it/products/netiq-sentinel/contact.

Installazione di Sentinel 8.5

Per informazioni sull'installazione di Sentinel 8.5, vedere la *Guida all'installazione e alla configurazione di Sentinel*.

Nota: Tutti gli host utilizzati per il server Sentinel e i relativi componenti devono essere configurati in un ambiente in grado di risolvere gli indirizzi DNS in modo bidirezionale (da nome host a IP e da IP a nome host).

Upgrade a Sentinel 8.5

È possibile eseguire l'upgrade a Sentinel 8.5 da qualsiasi versione precedente (a partire da Sentinel 8.2).

Importante: In seguito all'upgrade alla versione più recente di JDK, per configurare LDAPS e SDK, al posto dell'indirizzo IP l'utente deve utilizzare il nome host che sia anche risolvibile.

Importante: È stata apportata una modifica alla procedura di upgrade dell'installazione tradizionale e dell'applicazione. Fare riferimento a Impostazioni in Elasticsearch per la comunicazione cluster sicura e attenersi alla procedura descritta. Questa procedura è applicabile solo se si sta eseguendo l'upgrade di Sentinel alle versioni più recenti della versione 8.3.1 e precedenti.

Importante: È possibile eseguire un aggiornamento offline effettuando il download dell'immagine ISO delle patch offline per ciascuna applicazione. Per ulteriori informazioni, vedere Esecuzione di aggiornamenti offline.

Avviso: Se si esegue l'upgrade da versioni precedenti a Sentinel 8.3, sarà necessario assegnare manualmente l'autorizzazione **Invia eventi e allegati** agli utenti non amministratori che inviano eventi o allegati a Sentinel. A meno che non venga assegnata questa autorizzazione, Sentinel non riceverà più eventi e allegati da Change Guardian e Secure Configuration Manager.

Per l'installazione tradizionale, fare riferimento alla sezione Upgrade del sistema operativo nella *Guida all'installazione e alla configurazione di Sentinel*.

Problemi noti

Micro Focus si impegna affinché i propri prodotti forniscano soluzioni di qualità in grado di soddisfare le esigenze software delle aziende. I seguenti problemi noti sono attualmente in fase di studio. Per ulteriore assistenza su un problema, rivolgersi al supporto tecnico.

L'aggiornamento Java 8 incluso in Sentinel potrebbe avere ripercussioni sui seguenti plug-in:

- Connettore Cisco SDEE
- Connettore (XAL) SAP
- Integratore Remedy

Per eventuali problemi con tali plug-in, Micro Focus definirà le priorità e correggerà gli errori in base alle policy standard di gestione dei difetti. Per ulteriori informazioni sulle policy di supporto, vedere la pagina relativa alle policy di supporto.

Non è possibile visualizzare il grafico di previsione della capacità di memorizzazione

Problema: in **Sentinel Main** > **Memorizzazione** > **Stato**, il grafico **Previsione capacità memorizzazione primaria** non è disponibile. Ciò è dovuto al fatto che Zulu OpenJDK non include i font necessari.

Soluzione: per installare i font, utilizzare i comandi seguenti:

- yum install fontconfig
- yum install dejavu

Errore durante l'avvio di un dashboard Kibana dopo l'esecuzione dell'upgrade di Sentinel

Problema: l'avvio di un dashboard Kibana visualizza il seguente messaggio: `No default index pattern. You must select or create one to continue (Nessuno schema di indice di default. È necessario selezionarne o crearne uno per continuare).`

Soluzione: per impostare uno schema di indice di Kibana come schema di indice di default:

1. Selezionare una delle seguenti opzioni:
   - alerts.alerts
   - security.events.normalized_*
2. Fare clic su **Imposta come default**.

Non è possibile copiare i collegamenti agli avvisi di tutti gli avvisi in una vista avvisi in Mozilla Firefox e Microsoft Edge

Problema: l'opzione **Seleziona tutto*<numero di avvisi>* Avvisi** > **Copia collegamento avviso** non funziona in Firefox ed Edge.

Soluzione: eseguire i passaggi seguenti:

1. Selezionare manualmente tutti gli avvisi in ciascuna pagina della vista degli avvisi mediante la casella di controllo che consente di selezionare tutti gli avvisi.

2. Fare clic su **Copia collegamento avviso**.
3. Incollare nell'applicazione desiderata.

L'installazione di Sentinel, Collector Manager e Correlation Engine come immagine di applicazione OVF non visualizza la schermata di login

Problema: il programma di installazione si interrompe nella schermata di installazione in corso e non visualizza la schermata di login anche se l'installazione è stata completata.

Soluzione: riavviare la macchina virtuale e avviare Sentinel, Collector Manager o Correlation Engine.

L'applicazione Sentinel 8.2 in Microsoft Hyper-V Server 2016 non si avvia quando si esegue il riavvio

Problema: in Hyper-V Server 2016 l'applicazione Sentinel non si avvia quando se ne esegue il riavvio e viene visualizzato il seguente messaggio:

```
A start job is running for dev-disk-by\..
```

Questo problema si verifica perché il sistema operativo modifica lo UUID del disco durante l'installazione. Di conseguenza, durante il riavvio non riesce a trovare il disco.

Soluzione: modificare manualmente il disco UUID. Per ulteriori informazioni, vedere l'articolo 7023143 della knowledge base.

Errore durante l'upgrade a Sentinel 8.2 ad alta disponibilità.

Problema: quando si esegue l'upgrade all'applicazione Sentinel 8.2 ad alta disponibilità, Sentinel visualizza il seguente messaggio di errore:

```
Installation of novell-SentinelSI-db-8.2.0.0-<version> failed:
with --nodeps --force) Error: Subprocess failed. Error: RPM failed: Command exited
with status 1.
Abort, retry, ignore? [a/r/i] (a):
```

Soluzione: prima di rispondere alla richiesta riportata sopra, completare le operazioni seguenti:

1. Avviare un'altra sessione utilizzando PuTTY o un software simile all'host in cui si sta eseguendo l'upgrade.
2. Aggiungere la voce riportata di seguito al file `/etc/csync2/csync2.cfg`:

   `/etc/opt/novell/sentinel/config/configuration.properties`
3. Rimuovere la cartella di `sentinel` da `/var/opt/novell`:

   `rm -rf /var/opt/novell/sentinel`
4. Tornare alla sessione in cui è stato avviato l'upgrade e immettere `r` per procedere con l'upgrade.

L'installazione delle applicazioni Collector Manager e Correlation Engine ha esito negativo nella modalità MFA in caso di lingue diverse dell'inglese

Problema: l'installazione delle applicazioni Collector Manager e Correlation Engine ha esito negativo nella modalità MFA se la lingua del sistema operativo non è l'inglese.

Soluzione: installare le applicazioni Collector Manager e Correlation Engine utilizzando la lingua inglese. Al termine dell'installazione, modificare l'impostazione della lingua secondo necessità.

Problemi relativi a semplicità di usabilità nelle schermate di installazione dell'applicazione

Problema: i pulsanti **Avanti** e **Indietro** nelle schermate di installazione dell'applicazione non vengono visualizzati o, in alcuni casi, sono disabilitati, ad esempio:

- Quando fa clic su **Indietro** dalla schermata di verifica preliminare di Sentinel per modificare o rivedere le informazioni della schermata delle impostazioni di Sentinel, non è visualizzato alcun pulsante **Avanti** per proseguire l'installazione. Il pulsante **Avanti** consente di modificare solo le informazioni specificate.
- Se sono state specificate impostazioni di rete non corrette, la schermata di verifica preliminare di Sentinel indica che non è possibile procedere con l'installazione a causa di informazioni di rete errate. Non è visualizzato alcun pulsante **Indietro** per tornare alla schermata precedente e modificare le impostazioni di rete.

Soluzione: riavviare l'installazione dell'applicazione.

Collector Manager esaurisce la memoria se la sincronizzazione dell'orario è abilitata in Open-vm-tools

Problema: se si installa e si abilita manualmente la sincronizzazione dell'orario negli open-vm-tools, questi eseguono periodicamente la sincronizzazione dell'orario tra l'applicazione Sentinel (guest) e il server VMware ESX (host). Le sincronizzazioni dell'orario possono far sì che l'orologio del guest rimanga indietro o vada in avanti rispetto all'orario del server ESX. Fino a quando l'orario è sincronizzato tra l'applicazione Sentinel (guest) e il server ESX (host), Sentinel non elabora gli eventi. Di conseguenza, un numero elevato di eventi viene messo in coda in Collector Manager, il quale può infine rilasciare gli eventi una volta raggiunta la soglia. Per evitare questo problema, Sentinel disabilita di default la sincronizzazione dell'orario nella versione di open-vm-tools disponibile in Sentinel.

Soluzione: disabilitare la sincronizzazione dell'orario. Per ulteriori informazioni su come disabilitare la sincronizzazione dell'orario, vedere Disabilitazione della sincronizzazione dell'orario.

Quando la modalità FIPS 140-2 è abilitata, per Agent Manager è necessario utilizzare l'autenticazione SQL

Problema: quando in Sentinel è abilitata la modalità FIPS 140-2, l'utilizzo dell'autenticazione Windows per Gestione agenti causa un errore di sincronizzazione con il database di Gestione agenti.

Soluzione: utilizzare l'autenticazione SQL per Gestione agenti.

Durante l'installazione di Sentinel con configurazione ad alta disponibilità in modalità non FIPS 140-2 viene visualizzato un errore

Problema: l'installazione di Sentinel ad alta disponibilità in modalità non FIPS 140-2 viene eseguita correttamente ma appare per due volte l'errore seguente:

```
/opt/novell/sentinel/setup/configure.sh: line 1045: [: too many arguments
```

Soluzione: si tratta di un errore previsto che può essere ignorato. Anche se il programma di installazione visualizza un errore, la configurazione ad alta disponibilità di Sentinel funziona correttamente in modalità non FIPS 140-2.

Il comando Keytool visualizza un avviso

Problema: quando si utilizza il comando Keytool, viene visualizzato l'avviso seguente:

```
The JKS keystore uses a proprietary format. It is recommended to migrate to
PKCS12which is an
industry standard format using "keytool -importkeystore -srckeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -destkeystore
 /<sentinel_installation_path>/etc/opt/novell/sentinel/config/
.webserverkeystore.jks -deststoretype pkcs12".
```

Soluzione: si tratta di un avviso previsto che può essere ignorato. Anche se viene visualizzato l'avviso, il comando Keytool funziona come previsto.

Sentinel non elabora i feed di Threat Intelligence in modalità FIPS

Problema: in modalità FIPS, quando si elaborano feed pronti all'uso di Threat Intelligence provenienti da URL, in Sentinel viene visualizzato il seguente errore: `Received fatal alert: protocol_version`. Questo problema si verifica poiché i feed di minacce pronti all'uso ora supportano solo TLS 1.2, che non funziona nella modalità FIPS.

Soluzione: effettuare le operazioni seguenti:

1. Fare clic su **Sentinel Main** > **Integrazione** > **Origini di Threat Intelligence**.
2. Modificare l'URL per passare dal protocollo `http` ad `https`.

Il logout dall'applicazione principale Sentinel non esegue il logout dai dashboard e viceversa in modalità di autenticazione a più fattori

Problema: in modalità di autenticazione a più fattori, se si esegue il logout da **Sentinel Main** non si esegue il logout dai dashboard di Sentinel e viceversa. Ciò è dovuto a un problema in Advanced Authentication Framework.

Soluzione: in attesa che sia resa disponibile una correzione in Advanced Authentication Framework, aggiornare la schermata per visualizzare la schermata di login.

Il dashboard personalizzato Kibana non viene visualizzato dopo l'upgrade a Sentinel 8.3.1

Problema: il dashboard personalizzato Kibana non viene visualizzato quando si esegue l'upgrade da Sentinel 8.3 o versioni precedenti a Sentinel 8.3.1.

Soluzione: assicurarsi di aver ricreato il dashboard personalizzato dopo aver eseguito l'upgrade a Sentinel.

All'avvio di Kibana viene visualizzato il messaggio di errore di conflitto

Problema: dopo l'installazione o l'upgrade di Sentinel e al primo avvio di Kibana, viene visualizzato il messaggio di errore di conflitto.

Soluzione: ignorare il messaggio di errore di conflitto in quanto non ha alcun impatto sulle funzionalità.

Quando si riavvia il sistema operativo Redhat 8.1 e 8.2, Sentinel non viene avviato automaticamente

Problema: dopo aver installato Sentinel in OS Redhat 8.1 e 8.2, Sentinel (Server, RCM o RCE) non viene avviato automaticamente dopo il riavvio.

Soluzione: modificare il valore di SELINUX in **SELINUX=disabled** nel file `/etc/selinux/config`.

Quando si apre la console di gestione dell'applicazione Sentinel, viene visualizzato un messaggio di errore

Problema: dopo aver eseguito l'upgrade a Sentinel 8.3, quando si tenta di aprire la console di gestione dell'applicazione Sentinel delle istanze di CE (Correlation Engine) o di CM (Collector Manager) dei server HA (ad alta disponibilità), viene visualizzato il messaggio di errore `Error 404 - Not found` (Errore 404 - Non trovato).

Soluzione: per ulteriori informazioni, fare riferimento al documento della Knowledge Base di Micro Focus.

Gli utenti a cui è assegnata l'autorizzazione di occultamento di Gestione possono comunque visualizzare la scheda Gestione nella pagina Kibana

Problema: dopo aver eseguito l'upgrade a Sentinel 8.4, gli utenti cui è assegnata l'autorizzazione di occultamento di Gestione possono comunque visualizzare la scheda Gestione nella pagina Kibana ma non possono accedere alle funzioni della scheda Gestione.

Quando l'amministratore modifica il ruolo utente degli avvisi, le modifiche non vengono aggiornate immediatamente nella pagina Kibana

Problema: gli utenti esistenti non sono in grado di visualizzare immediatamente gli avvisi nella pagina Kibana, sebbene l'autorizzazione sia aggiornata dall'amministratore per la visualizzazione degli avvisi.

Soluzione: quando l'autorizzazione utente viene aggiornata, è necessario eseguire il logout e nuovamente il login.

Quando si avvia il dashboard di visualizzazione come utente tenant, viene visualizzato un messaggio di errore

Problema: quando un utente tenant non di default avvia il dashboard di visualizzazione, viene visualizzato un messaggio di errore **Forbidden** (Vietato). Questo messaggio di errore viene visualizzato ogni volta che il dashboard viene avviato dall'utente tenant non di default che dispone dell'autorizzazione di **sola visualizzazione** per l'opzione **Gestione** e non è presente alcun utente con autorizzazione di **modifica** per l'opzione **Gestione** in tale tenant.

Soluzione: ignorare il messaggio di errore in quanto non ha alcun impatto sulle funzionalità.

In RHEL, RCM e RCE non si connettono al server quando è abilitato CRL

Problema: l'istanza di Remote Collector Manager (RCM) and Remote Correlation Engine (RCE) non è in grado di connettersi al server quando in RHEL è abilitato CRL.

Soluzione: eseguire l'upgrade della **versione cURL** sul computer alla versione 7.60 o successiva.

RCM non inoltra gli eventi al server Sentinel quando sono abilitati i servizi di visualizzazione degli eventi, FIPS e CRL

Problema: nella nuova installazione della configurazione distribuita, dopo aver abilitato i servizi di visualizzazione degli eventi, FIPS e CRL, l'istanza di Remote Collector Manager (RCM) non inoltra gli eventi al server Sentinel.

Soluzione: se sono abilitati i servizi di visualizzazione degli eventi e FIPS o di visualizzazione degli eventi e CRL, l'istanza di RCM inoltra gli eventi al server Sentinel.

I rapporti sul caso non vanno a buon fine e generano eccezioni dopo l'upgrade del sistema operativo da una qualsiasi versione precedente alla versione più recente

Problema: quando si esegue l'upgrade del sistema operativo da una versione precedente alla versione più recente, i rapporti sui caso hanno esito negativo e generano eccezioni.

L'eccezione viene registrata durante il primo tentativo di reindicizzazione

Problema: viene registrata un'eccezione quando l'operazione di reindicizzazione viene eseguita per la prima volta.

Errore durante l'esecuzione di `convert_to_fips.sh` nella build dell'applicazione RCM/RCE di Sentinel 8.5

Problema: quando l'amministratore di sistema esegue `convert_to_fips.sh` nella build dell'applicazione RCM/RCE di Sentinel 8.5, dopo aver fornito le credenziali corrette degli utenti in un ciclo continuo, viene visualizzato il seguente messaggio di errore:

```
ERROR: Failed to connect to <Sentinel server IP>:
Failed to retrieve token for communication channel.
```

Soluzione: eseguire i passaggi seguenti:

1. Uscire dall'esecuzione dello script.
2. Accedere a `<percorso di installazione di RCM/RCE di Sentinel>/etc/opt/novell/sentinel/config/configuration.properties`
3. Impostare il valore di `rest.endpoint.port` alla porta del server Web corrispondente.

   Ad esempio, `rest.endpoint.port=8443`
4. Eseguire nuovamente `convert_to_fips.sh`

Contatti di Micro Focus

Per problemi specifici del prodotto, visitare la pagina di assistenza di Micro Focus all'indirizzo https://www.microfocus.com/it-it/support.

Ulteriori informazioni tecniche o suggerimenti sono disponibili da diverse origini:

- Documentazione del prodotto, articoli della knowledge base e video: https://www.microfocus.com/it-it/support
- Pagine della Comunità Micro Focus: https://www.microfocus.com/communities/

Note legali